

Policía Nacional de Colombia
Dirección de Investigación Criminal e INTERPOL
Frente de Seguridad Empresarial

Guía de Seguridad para los **Actores** de la **Cadena** de **Suministro**

Herramienta práctica para
la prevención criminal

2016

Ministerio de Defensa Nacional
Policía Nacional de Colombia

ISBN 978-958-98894-6-6



V Edición

General

Jorge Hernando Nieto Rojas

Director General Policía Nacional

Mayor General

Ricardo Alberto Restrepo Londoño

Subdirector General Policía Nacional

Mayor General

Jorge Enrique Rodríguez Peralta

Director de Seguridad Ciudadana

Mayor General

Carlos Ramiro Mena Bravo

Inspector General

Brigadier General

Fabián Laurence Cárdenas Leonel

Jefe Oficina de Planeación

Coronel

Luis Humberto Poveda Zapata

Director de Investigación Criminal e INTERPOL

Coronel

Pablo Ferney Ruiz Garzón

Subdirector de Investigación Criminal

Coronel

Juan Miguel Rojas Isaza

Jefe de Investigación Judicial

Mayor

Gelga Buitrago Martínez

Jefe Área de Asistencia y Cooperación para la Investigación Judicial y Frentes de Seguridad Empresarial

Corrección de Estilo

Roberto Sepúlveda

Agenda Pública Comunicaciones

Diseño e Impresión

Comercializadora COMSILA S.A.S.

Bogotá D.C., Colombia, Septiembre de 2016

AGRADECIMIENTOS

A todas las personas e instituciones que de manera activa aportaron y contribuyeron en la elaboración de la V Edición de esta Guía, que tiene como propósito entregar a los empresarios de Colombia, una vez más, una herramienta práctica para la prevención criminal, y así realizar una gestión eficiente de los riesgos asociados a la seguridad.

A los integrantes del Comité Editorial, que elaboraron, redactaron y consolidaron el contenido de este documento: a la señora Mayor Gelga Buitrago Martínez, Jefe Área Asistencia y Cooperación para Investigación Judicial; al doctor Enrique Rodero Trujillo, Investigador, docente y consultor en Prospectiva Estratégica; ingeniero John Jairo Mónoga González, Auditor Internacional de BASC; señores Intendente Hernando Rojas Balaguera y Subintendente Pedro José Mujica Gavilán, Jefes procesos de vinculación y análisis del Frente de Seguridad Empresarial.

De manera especial, a BASC Bogotá - Colombia; al Instituto Colombiano de Normas Técnicas y Certificaciones, ICONTEC; Cámara Colombiana del Libro; Jefatura de análisis y administración de información criminal de la DIJIN; Federación de aseguradores colombianos, FASECOLDA; multinacional Occidental de Colombia OXI; al Consejo de Seguridad en Cadena de Suministro de México; al equipo de trabajo del Frente de Seguridad Empresarial y empresarios que participaron con su aporte.

C O N T E N I D O

AGRADECIMIENTOS	3
PRÓLOGO	6
INTRODUCCIÓN	8
OBJETIVOS	10

CAPÍTULO 1

COMPRESIÓN DEL CONTEXTO

1.1	Amenazas globales con incidencias regionales	14
1.2	Tendencias globales de la prevención criminal - Responsabilidad penal de las personas jurídicas	24
1.3	Identificación de los tipos penales que afectan la continuidad del negocio en Colombia y medidas de control	27
1.4	Entorno de la seguridad, riesgo actual y su impacto en la cadena de suministro	67
1.5	Perspectivas de la Seguridad empresarial	71
1.5.1	Desde la opinión de diferentes actores de la cadena de suministro	71
1.5.2	Desde el análisis criminológico del Observatorio del Delito de la Policía Nacional	78
1.5.3	Desde uno de los Sistemas de Gestión certificados por el sector privado (hallazgos frecuentes)	91
1.6	Aproximación prospectiva de riesgos sociales y criminales de atención empresarial	106

CAPÍTULO 2

BUENAS PRÁCTICAS, LECCIONES APRENDIDAS Y RECOMENDACIONES

2.1	El desarrollo de competencias del líder de seguridad en la cadena de suministro	110
2.2	La certificación para el aseguramiento de las cadenas de suministro	114
2.3	Buenas prácticas para la continuidad de los negocios, "Gestiones de la Seguridad"	118
2.4	Diez ideas para controlar los riesgos sociales y criminales en un escenario de posacuerdo	132





CAPÍTULO 3

CAPACIDADES DE RESPUESTA INSTITUCIONAL

- | | | |
|-------|---|------------|
| 3.1 | Conceptualización de la prevención y su desarrollo en la Policía Nacional | 136 |
| 3.2 | Red de prevención criminal para el posacuerdo | 143 |
| 3.3 | Otras capacidades institucionales de apoyo a los empresarios | 156 |
| 3.3.1 | Red de apoyo - Dirección de Seguridad Ciudadana | 156 |
| 3.3.2 | RISTRA Red Integral para el Transporte - Dirección de Tránsito y Transporte | 157 |
| 3.3.3 | Programa Yo no pago, Yo denuncio - Dirección Antisecuestro y Antiextorsión | 160 |
| 3.3.4 | Programas de prevención - Dirección Antinarcoóticos | 163 |

CAPÍTULO 4

MARCO NORMATIVO

- | | | |
|-----|--|------------|
| 4.1 | Requisitos legales aplicables a algunos actores de la cadena de suministro | 166 |
| 4.2 | Nuevo Código Nacional de Policía y Convivencia - Ley 1801 del 29-07-16 | 171 |



Ceremonia de condecoración a directivos gremiales del Frente de Seguridad



PRÓLOGO

Colombia pasa por un momento histórico y una oportunidad coyuntural que impone retos y desafíos, tanto al sector público como privado, invitando a trabajar de manera conjunta y en red hacia un mismo objetivo. Más allá de la firma de un acuerdo de paz, repensar, generar inclusión, promover la reconciliación y la construcción de una sociedad más equitativa, es una responsabilidad que involucra a todos los actores de la sociedad; de tal forma, que se logren beneficios colectivos, entre otras garantías de convivencia y seguridad ciudadana, como insumo esencial de una paz sostenible.

La Policía Nacional es consciente de esta responsabilidad y se encuentra preparada en una primera visión 2030, para construir la transición y trabajar en pro del desarrollo sostenible del país, perfilando una planeación estratégica que exige compromiso a través de una hoja de ruta hacia el posacuerdo, la cual parte de la formulación del Plan Estratégico Institucional “Comunidades Seguras y en Paz”. En este sentido, desde nuestro proceso de modernización y transformación, la institución ha adoptado un enfoque diferencial de servicio en entornos urbanos y rurales, asumiendo nuevas dinámicas sociales, que incluye la lucha contra el crimen organizado y en general todas las modalidades delictivas que afectan el desarrollo económico, propiciando de esta forma, la continuidad y un clima favorable para los empresarios en Colombia.

Para garantizar este propósito, se han creado y fortalecido capacidades institucionales, entre otras, el Frente de Seguridad Empresarial DIJIN, el cual se entrega desde hace ya 16 años a la comunidad empresarial en

Colombia, como una herramienta estratégica para reducir sus niveles de victimización y aportar a la normalización del país, a partir de la promoción de la prevención criminal y el mejoramiento de la gestión del riesgo; en el marco de su interacción en las cadenas de suministro y/o de valor, así como su papel protagónico en la construcción de la paz con seguridad.

Desde esta perspectiva, es importante repensar las políticas de seguridad empresarial, las cuales incluyen planes corporativos para asegurar procesos, información, operación, instalaciones y demás activos, a través de una mejor capacidad para identificar la transformación del crimen y sus actores, que permitan adaptar sus mapas de riesgos, así como diseñar una nueva arquitectura social estratégica, planes de voluntariado corporativo, a partir de la definición de un nuevo pero lógico mapa social, que se extienda a encadenamientos y compras inclusivas, sostenibles y de gran impacto, alineadas con la rentabilidad y competitividad de su negocio.

De 17 Objetivos de Desarrollo Sostenible promovidos por Naciones Unidas, el número 16, "Paz, justicia e instituciones sólidas, nos remite a escenarios múltiples para la paz, escenarios ligados al progreso de la democracia, de las libertades políticas, de los derechos fundamentales, sociales, económicos, culturales y ambientales. Para lograr este propósito se requiere la interacción de diversos actores que hacen posible sociedades pacíficas e inclusivas para el desarrollo sostenible".

De esta manera, nuestra institución está alineada y le apunta a ofrecer todo su compromiso, integrándose con el fortalecimiento de la prevención criminal a través de herramientas como el entregable de la Guía de Seguridad para los Actores de la Cadena de Suministro, producto investigativo que se une a otros que marcan la gestión institucional de esta vigencia, tales como la implementación de herramientas de convivencia, especialmente del Código Nacional de Policía; así como el fortalecimiento de la investigación criminal para reducir la impunidad en la justicia; todas apuntando a garantizar el cumplimiento de la misión constitucional de la Policía Nacional de los colombianos.

General JORGE HERNANDO NIETO ROJAS
Director General de la Policía Nacional



INTRODUCCIÓN

Teniendo en cuenta el Plan Estratégico Institucional y los contenidos del Manual del Sistema de Gestión Integral, “la Policía Nacional tiene el compromiso de contribuir al mejoramiento de las condiciones de seguridad y convivencia ciudadana del país, de ser una Institución confiable y respetada, soportada en el comportamiento ético de sus integrantes; posicionándose como una entidad integrada con la comunidad, en la decisión de construir las realidades de una convivencia pacífica y segura, desde la perspectiva que ofrece la corresponsabilidad social y la legitimidad organizacional”.

A partir de este marco, hace 16 años, la Dirección de Investigación Criminal e INTERPOL, desde su capacidad investigativa, ha desarrollado su función incorporando la prevención criminal como un proceso estratégico que despliega en su oferta de valor sinergia focalizada y diferencial de trabajo en red con los empresarios y gremios en Colombia; orientada a reducir los índices de criminalidad que los afectan frecuentemente, a partir de la concepción de realizar una eficiente gestión del riesgo y la aplicación de controles efectivos que permitan anticipar los eventos de victimización y perseguir de manera conjunta al victimario, es decir, al actor de modelos de economía criminal que afectan el patrimonio económico.

Esta gestión ha venido realizándose con éxito, a través del Frente de Seguridad Empresarial, el cual articula y pone a disposición de los empresarios todas las capacidades policiales de la institución, coordinando esfuerzos para garantizar mayor seguridad a los promotores del desarrollo económico, y en este sentido, a las cadenas de valor, en las cuales sus actores imprimen esfuerzos de competitividad y crecimiento, gracias a las condiciones de convivencia y seguridad.

Para materializar este trabajo conjunto, como evidencia de esos lazos de confianza e intercambio de información con todos los sectores productivos del país y más de 1.800 empresarios que hacen parte de esta alianza público – privada, trianualmente se entrega, como en esta oportunidad, la Guía de Seguridad para los Actores de la Cadena de Suministro. Esta publicación, en su quinta edición, se presenta como parte

de una colección única que simboliza precisamente esa construcción conjunta e incluyente, posicionada por la evolución de sus contenidos, por los aportes que hace en la identificación de los riesgos asociados a seguridad en cada proceso de la empresa; de tal forma, que se adopten controles que garanticen la continuidad del negocio.

Esta versión entrega a todos los lectores, con el concurso de profesionales e instituciones expertas que se unieron a este trabajo, a quienes extendemos nuestros agradecimientos, una investigación compuesta en un primer capítulo por un contexto de la seguridad desde una visión global, latinoamericana o regional, para fijar su atención en un diagnóstico local de la seguridad, a partir de la identificación de los tipos penales (Ley 599 del 2000), que afectan la continuidad de negocios en Colombia y las medidas de control, desde la perspectiva de la seguridad empresarial, obtenida a través de la aplicación de una herramienta tipo encuesta a una muestra de empresarios, desde el Observatorio de Criminalidad de la Policía Nacional a partir del análisis criminológico de la victimización a este mismo segmento de la población, desde los Sistemas de Gestión certificados por el sector privado, identificando los hallazgos frecuentes y desde las dinámicas actuales de cara a los retos y desafíos que impone el posacuerdo.

El lector encontrará en un segundo capítulo, la conceptualización de la prevención y su desarrollo en la Policía Nacional, así como las capacidades institucionales con acceso disponible para los empresarios desde las diferentes modalidades del servicio policial, lo que va a permitir conocer el portafolio, actividades de prevención y protocolos de reacción; posteriormente, contará con información de buenas prácticas y recomendaciones a partir de lecciones aprendidas, los aportes de ICONTEC, desde su experiencia como ente certificador, comentando la norma ISO 28000 para la seguridad en cadenas de suministro y finalmente ofrecer información que permita actualizar al lector de lo que puede victimizarlo, con el fin de lograr desarrollar una mayor capacidad de resiliencia.

En un tercer capítulo, este esfuerzo presenta el valor agregado más importante; la entrega de programas de seguridad para garantizar la continuidad de los negocios, cuando se materializan riesgos asociados a la seguridad. Finalmente, encontrarán el marco normativo aplicable a los diferentes sectores productivos en Colombia, dando importancia a la legitimidad y cultura de la legalidad desde el sector privado.

Esto no solo recaba sobre la corresponsabilidad, sino también en la necesidad de tener una activa participación como actor social altamente participativo, como parte del conjunto de estrategias orientadas a reducir la probabilidad de ocurrencia de delitos y formas de violencia.

Coronel LUIS HUMBERTO POVEDA ZAPATA
Director de Investigación Criminal e INTERPOL

OBJETIVOS DE LA GUÍA

General

Brindar a los diferentes actores de la cadena de suministro una herramienta práctica de consulta que permita fortalecer la prevención criminal, a partir del conocimiento del contexto y la perspectiva actual de la seguridad desde diferentes ópticas, así como planes de continuidad de negocio que fortalezcan la gestión del riesgo y la seguridad asociada a procesos, operación, personas, información, instalaciones y demás activos de una empresa, impactando la misión y objetivos estratégicos institucionales.

Específicos

- › Aportar información para identificar en el contexto, amenazas de seguridad a nivel global, regional y local.
- › Identificar las capacidades de respuesta institucional para apoyar la gestión de la seguridad empresarial, a partir de la prevención criminal y la reacción eficiente.
- › Posicionar el Frente de Seguridad Empresarial como una red para la prevención criminal en el posacuerdo, respaldado la legitimidad, la confianza y las relaciones funcionales con las instituciones públicas.
- › Proponer buenas prácticas y/o gestiones de seguridad a los empresarios en Colombia, que permitan controlar los eventos que impactan negativamente el desarrollo de sus actividades.
- › Identificar los requisitos legales aplicables a algunos actores de la cadena de suministro.
- › Ofrecer información que permita un mayor nivel de adaptación del sector privado a los retos y desafíos que impone el posacuerdo, con el fin de construir un país más seguro y competitivo.

ABREVIATURAS

BASC	Business Alliance for Secure Commerce
DITRA	Dirección de Tránsito y Transporte
DIRAN	Dirección de Antinarcóticos
DIJIN	Dirección de Investigación Criminal e INTERPOL
FESEM	Frente de Seguridad Empresarial DIJIN
ISO	International Organization for Standardization
POLFA	Policía Fiscal y Aduanera
SIPLAFT	Sistema Integral para la Prevención del Lavado de Activos y de la Financiación del Terrorismo
SARLAFT	Sistema de Administración del Riesgo del Lavado de Activos y Financiación del Terrorismo
OFAC	Oficina para el Control de Activos Extranjeros
UIAF	Unidad de Información y Análisis Financiero
RUAF	Registro Único de Afiliados
FOSYGA	Fondo de Solidaridad y Garantía
INTERPOL	International Criminal Police Organization
DEA	Drug Enforcement Administration
ROS	Reporte de Operaciones Sospechosas
RUES	Registro Único Empresarial y Social
DHS	United States Department of Homeland Security
RUNT	Registro Único Nacional de Tránsito
CCTV	Círculo cerrado de televisión

TABLA DE AUTORES

1	Mayor Gelga Buitrago Martínez	Jefe Área Asistencia y Cooperación para policía judicial y FSE - DIJIN	Aproximación prospectiva de riesgos sociales, criminales de atención empresarial y medidas de prevención
2	Doctor Doctor Miguel Velásquez Olea	Director Ejecutivo BASC Bogotá - Colombia	Sistemas de Gestión certificados por el sector privado (hallazgos frecuentes)
3	Intendente Hernando Rojas Balaguera	Jefe proceso de vinculación FSE - DIJIN	Identificación de los tipos penales que afectan la continuación del negocio en Colombia y medidas de control
4	Intendente Hernán Alfonso Ramírez Rodríguez	Responsable de articulación del servicio en prevención Dirección de Seguridad Ciudadana	Conceptualización de la prevención y su desarrollo en la Policía Nacional
5	Ingeniero John Jairo Mónica González	Auditor Internacional BASC	Buenas prácticas para la Gestión de la Seguridad
6	Maestro Enrique Rodero Trujillo	Investigador, Docente y Consultor en Prospectiva Estratégica	Las amenazas globales con incidencias regionales
7	Abogados Yuri Farfán Andrés Rodríguez	Asesores Jurídicos Cofecar Grupo OET	Marco Normativo de algunos actores de la cadena de suministro
8	Andrea Olaya Cañón	Centro de entrenamiento ICONTEC	La certificación para el aseguramiento de la cadena de suministro
9	Aristides Contreras F. Orlando Hernández Angarita	Presidente y Vicepresidente Ejecutivo Comunidad latinoamericana de consultores y asesores en Gestión de riesgos y seguridad, COLADCA	Entorno de la seguridad, riesgo actual y su impacto en la cadena de suministro
10	Subintendente Pedro Mujica Gavilan	Gestor Seguridad Empresarial	Diseño Gráfico
11	Doctor Eduardo Hernández Ruiz	Presidente del Consejo de Seguridad en Cadena de Suministro en México	El desarrollo de competencias del líder de seguridad en cadena de suministro

I

CAPÍTULO



Comprensión del Contexto

1. COMPRENSIÓN DEL CONTEXTO

1.1 Amenazas globales con incidencias regionales



“La tecnología es neutral, puede utilizarse para el bien y para el mal y aportará medios para cometer crímenes y para evitarlos, para cubrirlos y detectarlos.”



Según la Real Academia de la Lengua, la globalización es una tendencia de los mercados y las empresas a extenderse alcanzando una dimensión mundial, sobrepasando las fronteras nacionales, generando así procesos de intercambio que se aceleraron a comienzos del siglo XX, los cuales se han caracterizado por aportar grandes desarrollos a la humanidad, pero a su vez han dado pie a la creación de nuevos problemas comunes y la expansión o multiplicación de otros ya existentes en el mundo, como los procesos migratorios y la situación de los refugiados, el crecimiento excesivo de la población; la falta de desarrollo de las economías nacionales; la degradación de los sistemas ecológicos y del medio ambiente; todos ellos y sus derivaciones se configuran como amenazas transnacionales y constituyen factores de riesgo para los países y la comunidad internacional, ya que fueron abriendo la puerta a nuevas modalidades de comportamiento delictivo y por ende a lo que denominamos como nuevas amenazas de carácter transnacional, a menudo protagonizadas por agentes no estatales, que nos cuestionaron los límites tradicionales entre la seguridad exterior y la seguridad interior de un país.

Todo esto ha puesto en evidencia la estrecha interrelación que existe entre los problemas económicos, políticos, sociales y medioambientales con los problemas de seguridad, sumado al momento histórico en que se encuentra el país concretando el acuerdo de paz con las FARC y la refrendación por parte del pueblo colombiano, a través del plebiscito de dichos acuerdos; por eso, en este sucinto escrito se presentará un paneo de las principales amenazas globales que podrán afectar el desempeño futuro de cualquier organización empresarial, según su sector de desempeño, en un futuro escenario de posacuerdo en Colombia.

Las amenazas globales, en la realidad son fenómenos sistémicos que se interrelacionan para complementarse unos con otros, pero para su

comprensión podríamos exponerlos en tres grupos: los **factores contribuyentes o generadores de amenazas potenciales**, el **crimen transnacional** propiamente dicho y **desastres naturales y accidentes catastróficos** en el medio ambiente que afectan la seguridad.

A. Factores contribuyentes o generadores de amenazas potenciales

Los factores contribuyentes son aspectos sociales que sin ser delitos en sí mismos, se convierten en factores de riesgo real o potencial para que se consoliden delitos, algunos de ellos son:

- **Crecimiento de la población: proyección al año 2100:** Hoy tenemos más de **7.200 millones** de seres humanos en la Tierra. En 2030, habrá más de **8 mil millones**. Para 2050 la cifra se aproximará a los **9 mil millones**.

Este enorme aumento de la población planteará serios problemas en todas las naciones del mundo. La gestión global de 9 billones de personas y la exigencia de tratamiento médico, comida, trabajo, alojamiento y seguridad, será el desafío más angustiante al que ninguna civilización se haya enfrentado nunca (Canton, 2006).

- **Pobreza, indigencia y desigualdad:** La pobreza extrema y la exclusión social de amplios sectores de la población, erosiona la cohesión social y

vulnera la seguridad de los Estados, afectando la estabilidad económica y la democracia.

Las naciones y empresas más ricas deberán construir una **globalización ética y sostenible** preocupándose por la gente con la que comercian y el medio ambiente en que comercian o tendrán que construir barricadas para rechazar a todos aquellos a los que han desposeído.

James Canton en *The extreme future* plantea que "La gente que ya no tiene esperanza en el futuro, es la más peligrosa del mundo", ya que haría cualquier cosa para conseguir ese futuro o para destruir a quienes considera que se lo están robando. Por lo cual, cualquier empresa con visión debe abordar un real y conciente proceso de responsabilidad social que fortalezca sus grupos de interés.

- **Aceleración del desarrollo tecnológico:** durante los **próximos 25 años** habrá más evolución tecnológica que a lo largo de todo el siglo pasado. El científico Michio Kaku imagina un mundo en el que la mente controlará las computadoras, los coches podrán flotar sobre campos magnéticos, los lentes de contacto tendrán acceso a internet y los elevadores serán espaciales.

La mayor parte del Esquema de Valor Agregado, **EVA**, en bienes y servicios proviene del **conocimiento y la información incorporados**. La tecnología ha revolucionado los negocios, la rapidez generada es la nueva ventaja competitiva. La **innovación** de productos, de

procesos, servicios y negocios es la nueva estrategia de supervivencia de las organizaciones y la mayor parte de ella se soporta en desarrollo tecnológico.

Ray Kuzwell (2010), sostiene que uno o dos años más tarde de que las máquinas alcancen el nivel de la inteligencia humana, el desarrollo exponencial de la tecnología se traducirá en que esas máquinas dispongan de potencial para ser dos veces más “inteligentes” que los humanos. Luego, un año o poco más, cuadruplicarán la diferencia.

Para finales de 2017, **el 85% de la población mundial tendrá Internet móvil de alta velocidad**, el tráfico mundial de datos se multiplicará por 15, fusionándose en un nuevo “medio de comunicación” global: “siempre hablando, siempre conectados, todos con todos, todo con todo, en todo momento y por todas partes”. Esta súper-web multisensorial o internet de las cosas, creará experiencias virtuales que parecerán tan reales que será imposible distinguir las de las reales.

Para hacer frente a una sociedad que evoluciona hacia el no uso de efectivo serían necesarias nuevas leyes y nuevos métodos de hacerlas valer. El futuro demanda un tipo de cooperación interinstitucional público - privada más allá de lo conocido. Con una economía de alta velocidad y alta tecnología surgirán nuevas formas de crimen y de prevención criminal.

La tecnología es neutral, puede utilizarse para el bien y para el mal y aportará medios para cometer crímenes y para evitarlos, para cubrirlos y detectarlos.

Los problemas de fijación de precios, manipulación de mercados, intercambios de información privilegiada y otros tipos de engaños y fraudes crecerán y afectarán a más personas, así que, si su organización no sabía estas cosas, es mejor que se prepare y se anticipe a ello.

B. Crimen Transnacional

En el crimen transnacional encontramos las modalidades delictivas que más fuerza están tomando y pueden afectar el desempeño organizacional, especialmente en estos momentos en los que se avecinan cambios producto de los acuerdos de paz, entre ellas destacaremos algunas que se deben tener en cuenta:

1. Crimen organizado transnacional

La cuarta economía mundial no es China. En realidad, la cuarta economía mundial no es ningún país. Pero es una de las economías más dinámicas, productivas e innovadoras del mundo. Sus empresarios han aprovechado el aumento del comercio internacional, el desarrollo del sector financiero y la explosión de las nuevas tecnologías para convertirse en verdaderos motores del crecimiento en países de la talla de Rusia, China o Tailandia. Son capitalistas puros. Comercian con todo. Sus mercancías son armas, drogas, software, películas, discos y hasta seres humanos. Es la economía del crimen organizado.

Este fenómeno se puede diferenciar de otras organizaciones criminales por medio de tres características básicas: uno, la **Diversificación** de sus actividades que no son mutuamente excluyentes; dos, la **Transnacionalización** que trascienden las fronteras nacionales y, tres, la **Interacción** en redes globales y descentralizadas.

Se los puede clasificar en tráfico ilícitos (personas, drogas, armas, materiales, medicamentos, mercancías, alimentos, etc.) y delitos económicos. Los resultados de su accionar son diversos: distorsión del normal funcionamiento de los mecanismos de mercado y la efectividad de las normas legales; corrupción, cooptación y manipulación de empleados y funcionarios públicos; erosión de la credibilidad y reputación del Estado ante los inversores privados, externos e internos; en casos extremos, se desdibujan los límites entre las organizaciones criminales y el Estado.

Dadas las anteriores características y efectos, se dificulta la forma de contrarrestar su accionar. La ONU calcula que el **blanqueo o lavado de dinero** mueve alrededor de un billón de euros anuales. La movilidad del capital, además, refuerza las posibilidades de inversión de los criminales.

La delincuencia ha aprovechado los avances de la tecnología y las finanzas para globalizarse. Hoy, el crimen organizado mueve **2,5 billones de euros anuales**, es decir, entre el 2,5% y el 5% del PIB mundial (UNDOC).

2. Tráfico y consumo de drogas

Por tráfico de drogas se entiende no sólo cualquier acto aislado de transmisión del producto estupefaciente, sino también el transporte e incluso toda tenencia que, aun no implicando transmisión, suponga una cantidad que exceda de forma considerable las necesidades del propio consumo, ya que entonces se entiende que la tenencia tiene como finalidad promover, favorecer o facilitar el consumo ilícito (entendiéndose como ilícito todo consumo ajeno).

El narcotráfico seguirá siendo un negocio lucrativo y factor generador de otros delitos conexos para mantener su modus operandi, en la forma en que busca financiación (secuestro, extorsión), como genera su producto (cultivos ilícitos), lo distribuye (tráfico ilegal, mulas) y garantiza su mercado (microtráfico), etc.; de allí que algunos piensen en su legalización.

3. Secuestro, tráfico y trata de personas

Los nuevos comportamientos sexuales han provocado un boom del tráfico de mujeres y del turismo sexual. Según la *think tank* Federación de Asociaciones de Naciones Unidas, hoy, el tráfico de personas es ya el tercer sector del crimen organizado más grande, con una cifra de negocio anual de unos 28.000 millones de euros. Según la Organización Internacional de Migraciones, OIM, 4 millones de personas son prostituidas contra su voluntad en todo el mundo. De

ellas, el Fondo de las Naciones Unidas para la Infancia (UNICEF, 2011) estima que más de 2 millones son menores de edad.

Pero la trata de personas no solo atañe a temas de explotación sexual (principalmente niños, niñas y mujeres), sino que también apunta a esclavitud laboral para trabajos forzosos y en áreas como construcción, producción de bienes, agricultura, industria pesquera y servicio doméstico.

El tráfico y trata de personas no solo se da entre un país y otro, sino también en la parte interna de los países (traficando personas de zonas rurales pobres a zonas urbanas y centros turísticos) y también hacia y desde otras regiones y países del mundo. La Organización de las Naciones Unidas (ONU, 2011) asegura que es el tercer negocio más lucrativo a nivel mundial, después de las drogas y armas generando entre 8 y 10.000 millones de dólares al año (2014).

4. Delito cibernético

Según las estadísticas el **crimen tradicional disminuiría paulatinamente**, mientras que el crimen por medios informáticos y otros tipos de delitos tecnológicos aumentarían con el tiempo. El delito cibernético consiste en atacar sistemas informáticos, realizar piratería, fraude o falsificación y/o publicar contenidos ilegales en medios digitales o la nube. Este se ha convertido en una preocupación de carácter mundial. El inventario de daños y delitos causados por esta modalidad de crimen no es posible cuantificarlo con exactitud, no solo por la gran variedad de formas y modos de operación que han desarrollado los delincuentes, sino también por tratarse de una actividad que ocurre en casi todos lugares donde exista un computador, un teléfono móvil, o cualquier dispositivo con señal de internet o comunicación.

Las entidades financieras, entes particulares y del Estado, al igual que organizaciones de todo tipo, han sido víctimas de ciber-ataques, que buscan acabar no solo con el capital económico de los afectados sino también con su posición moral y su capital social.

Un estudio de Certicámara y la multinacional Symantec (2013) en Colombia, evidenció que cuatro de cada 10 usuarios de Internet, los cuales suman 8 millones, son víctimas de delitos por medios informáticos que van desde la simple violación de sus cuentas o correos hasta robos; respecto al impacto global del delito, agrega que a nivel mundial se presentan cerca de un millón de víctimas diarias y en Colombia 16.438 (6 millones al año). En promedio se denuncian 1.000 delitos informáticos al año, que van desde el acceso abusivo a un sistema informático, hurto por medios informáticos y semejantes, interceptación de datos informáticos, la violación de datos personales, la transferencia no consentida de activos, la suplantación de sitios web, el daño informático, el matoneo, la obstaculización ilegítima de un sistema

informático y la instalación de un programa informático empleado por los delincuentes para cifrar la información contenida en un computador y luego pedir recompensa.

Según las estadísticas sobre denuncias, el delito bancario más común es la clonación de tarjetas, principalmente en las ciudades de Bogotá, Cúcuta, Cartagena, Barranquilla, Medellín y Cali. Le siguen el 'phishing' (creación de páginas falsas para capturar información financiera de los clientes) y el 'smishing' (envío de mensajes de texto ofreciendo premios o solicitando a las personas comunicarse con un Centro de llamadas, que resulta ser falso).

Un sistema de clasificación interesante es el definido por el convenio sobre la ciberdelincuencia del Consejo de Europa (Council Europe Convention), en el que se distinguen cuatro diferentes tipos de infracciones: delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos informáticos; delitos relacionados con el contenido; delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

5. Destrucción del medio ambiente

Bajo este delito se cobijan muchos atentados contra el ecosistema y por ende contra la misma especie

humana, entre ellos: el tráfico de especies nativas o exóticas que va en crecimiento, minería ilegal que ayuda al lavado de activos y diversificar ingresos a las organizaciones criminales, deforestación en zonas de reserva para vender productos maderables a altos costos, entre otros.

El mundo cuenta con 30 millones de km² de bosques. Colombia ha llegado a talar hasta 500.000 hectáreas anualmente para cultivos ilícitos, madera, agricultura y minería. Hoy el costo de madera ilegal es equiparable al de algunas drogas ilícitas.

6. Conflictos o controversias limítrofes

Son aquellos fenómenos negativos que se presentan entre dos o más naciones cuando se cuestiona la soberanía de alguna de ellas en las zonas colindantes con sus vecinos, particularmente Colombia, en los últimos años se han venido dando como tendencia emergente el incremento de dichos fenómenos, que aunque vienen de años atrás; han cobrado más impulso por intereses políticos e ideológicos comerciales con nuestros vecinos, como es el caso de Nicaragua, el cual está en proceso de disputa y Venezuela, el cual se encuentra en proceso de resolución; a futuro podrían agravarse o aparecer nuevos conflictos de este tipo, generando inestabilidad en los negocios fronterizos y las exportaciones con países vecinos.

7. Terrorismo

Naciones Unidas define al terrorismo como “actos de violencia cometidos contra personas inocentes o no combatientes, con la intención de obtener fines políticos a través del terror y la intimidación”, y sus características principales son: 1. Nivel de clandestinidad; 2. Sorpresa; 3. Desproporción del daño o la destrucción; 4. Desinterés por la vida humana; 5. Fundamentalmente actúa sobre la población y no sobre los recursos; 6. Impregnación ideológica; 7. Uso indiscriminado de la fuerza; 8. Explotación psicosocial o comunicacional del hecho; 9. Reclamo de autoría; 10. Es indiscriminado en cuanto a sus víctimas.

Se constituye en una de las principales amenazas de naturaleza transnacional en el orden emergente de la posguerra fría. Su ambiente es generalmente urbano, a diferencia de la guerrilla que generalmente es rural, pero que paulatinamente se fue incorporando en lo urbano.

8. Corrupción

Los temas de corrupción y malversación de fondos que afectan la funcionalidad del Estado, sus finanzas públicas y el buen uso de los recursos, se contraponen a una gestión pulcra y eficiente de los funcionarios públicos.

En Colombia, tal vez, el crimen que más ha generado índices de violencia y delincuencia es la corrupción, profundamente ligada al status quo de nuestra cultura empresarial, que en muchos casos la ve como algo normal, parte de las negociaciones para obtener contratos, o a veces incluso, con pagos de millones de pesos en multas para llevarse miles de millones en ganancias, pero que no se percata de cómo en el largo plazo se menoscaba la sociedad y produce exclusión en su interior. Dicha sociedad excluida piensa cada vez más en el crimen como un medio para alcanzar una meta legítima. La corrupción es un factor germen de inestabilidad política e institucional e inestabilidad económica y desempleo.

9. Extorsión

La legislación define la extorsión como “El que constriña a otro a hacer, tolerar u omitir alguna cosa, con el propósito de obtener provecho ilícito o cualquier otra utilidad ilícita o beneficio ilícito, para sí o para un tercero...” (Código Penal, Ley 599 de 2000).

Es la capacidad de exigencia que tiene una persona de lograr a través de la presión psicológica o mediante vías de hecho, que su víctima vaya en contra de su capacidad volitiva, cognoscitiva y de autodeterminación para lograr un provecho o beneficio ilícito que usualmente es económico.

Actualmente, las modalidades más reconocidas son: microextorsión (exigencia de pequeñas cantidades); hurto extorsivo por devolución de bienes (a cambio del bien captado de manera ilícita, exigir una suma de dinero por su devolución); ciber-extorsión o de información íntima (apropiación de datos o imágenes dejados en las redes sociales o medios digitales a cambio de exigencias de carácter económico, sexual u otra clase de beneficios); extorsión clásica (hurto para obtener de su víctima un beneficio de gran cuantía económica) y carcelaria (realizada por celulares usados desde las prisiones por reclusos).

10. Deslocalización, mutación y flexibilización de las líneas de control jerárquico

Las organizaciones delincuenciales han venido paulatinamente entrando en un proceso de atomización, diversificación y deslocalización, en síntesis, podríamos decir flexibilidad, como respuesta a las estrategias de las organizaciones policiales locales y regionales; el caso más visible ha sido la fragmentación de los grandes carteles de la droga y su sustitución por organizaciones delictivas independientes de menor tamaño.

Saltanat Berdikieeva, analista de la consultora RiskMetrics y autora de varios artículos publicados en la revista especializada *Jane's*, sobre crimen organizado en Asia Central, sostiene que hoy “Cada vez hay menos organizaciones verticales,

es decir, grupos a la antigua usanza, que controlaban toda la línea de producción y comercialización. Ahora hay grupos pequeños, locales, que se coordinan entre sí. La mafia al estilo siciliano, en torno a un líder al que se jura fidelidad, ha desaparecido”.

C. Desastres naturales y accidentes catastróficos

Los desastres naturales y los de origen humano, el VIH/SIDA y otras enfermedades, otros riesgos a la salud y el deterioro del medio ambiente. Está claro que hay una brusca variación en las condiciones meteorológicas habituales del planeta y que supone un peligro para nuestras sociedades. En 1972 el Club de Roma advirtió sobre la grave crisis ambiental del siglo XXI.

Si se agravan las tormentas, si el nivel de los mares sube, si las inundaciones aumentan, si las sequías se prolongan y si las olas de calor se incrementan, millones de seres humanos tendrán que desplazarse y la sociedad empezará a descomponerse. Habrá refugiados en todas nuestras puertas. Prepararnos lo mejor posible para el cambio climático que viene. No podemos mantener el planeta sin una agricultura avanzada y acelerada si queremos evitar un futuro de hambre masiva.

Si cada uno de nosotros, en el mundo desarrollado, viviera teniendo en cuenta la factura medioambiental de su forma de vida y actividades empresariales, los objetivos en este aspecto podrían alcanzarse mucho más fácilmente. De aquí a 2030, un

escenario propone que todos habremos aprendido a conservar, a reciclar y a reutilizar, pues no tenemos elección. No ser responsables como consumidores, se habrá vuelto un crimen moral y quizá un crimen legal.

Entre los principales riesgos que presentan los desastres naturales encontramos: terremotos, huracanes, inundaciones, maremotos, accidentes catastróficos (ex: derrame de petróleo o residuos tóxicos).

- **La amenazante crisis energética por aumento de demanda**

Ahora, que vamos a llegar a ser 9 mil millones sobre la tierra, a mitad de siglo, buscando cada uno una mejor calidad de vida, habrá indudablemente una angustiosa necesidad de consumir más y más energía.

Los cálculos de nuestro consumo futuro de energía varían mucho, pero, como mínimo, pensamos que el consumo mundial aumentará un 50% de aquí a 2030, y la máxima previsión es de un aumento del 100%. Es probable, y casi cierto, que las energías de fuentes renovables y sostenibles proporcionarán la mayor parte de las necesidades mundiales en energía (siempre creciente) de aquí a 2030.

¿Por qué es tema la energía cuando se habla del futuro del crimen? El control sobre las fuentes de energía y los posibles robos de energía son dilemas emergentes, resultado del creciente costo de los energéticos; así como del temor de que las principales fuentes son escasas o están en peligro de llegar a precios que las mantendría fuera del alcance de la mayoría de los consumidores.

Como gran conclusión podríamos decir que todos estos factores que afectan la seguridad, se pueden convertir en grandes oportunidades para el desarrollo empresarial y sus alianzas con el sector público de seguridad.

Referencias Bibliográficas

- Aviles F., J. (2006). Las amenazas globales del siglo XXI, *Revista CSIC*, 2006.
- Canton, J. *Extreme Future*
- Hernández M., J. (2008). *El Crimen Organizado en América Latina y el Caribe: Mapeo del Caso Centroamericano*. Fundación Friedrich Ebert 24-26 de junio 2008, México D.F.
- Michio K. (2012). Cómo la ciencia determinará el destino de la humanidad y nuestra vida cotidiana en el siglo XXII. *Debate: México*.
- Programa de Naciones Unidas para el Desarrollo, PNUD (2007). *Informe de Desarrollo Humano 2014-2015*. New York, Estados Unidos.
- Seguridad y Crimen Organizado Transnacional, Fundación Konrad Adenauer y Red Centroamericana de Centros de Pensamiento e Incidencia - laRED - Febrero de 2011, Guatemala.

MG. ENRIQUE RODERO TRUJILLO

Investigador, Docente y Consultor en Prospectiva Estratégica

1.2 Tendencias globales de la prevención criminal - Responsabilidad penal de las personas jurídicas



“La prevención de delitos como eximente y atenuante de responsabilidad penal de las empresas”.

Este presupuesto jurídico surge de una corriente cada vez más aceptada a nivel global, en el que desde el sistema penal se promueve la adopción de Planes de Prevención Penal en las empresas, con fuentes y motivaciones que van desde la implementación y cumplimiento por: debida diligencia, buenas prácticas de asunción voluntaria, corresponsabilidad social empresarial, hasta eximentes y atenuantes de responsabilidad penal, en la comisión de conductas punibles, en consonancia de la integración en las jurisdicción legales internas correspondientes, con las directrices trazadas por convenciones adoptadas por los países miembros de organizaciones internacionales, como es el caso de Naciones Unidas (Colombia país miembro) y la Organización para la Cooperación y Desarrollo Económico, OCDE (Colombia adhesión), GAFI, entre otros, los cuales cuentan con medidas y lineamientos contra el delito transnacional y la corrupción, en las que se conmina por la adopción de figuras jurídicas que contemplen la responsabilidad penal de las personas jurídicas (empresas), en procura de contrarrestar el delito transnacional, como amenaza global.

Unión Europea

La responsabilidad penal de las personas jurídicas, igualmente, goza de admisibilidad en la mayor parte de los países de la unión europea; que en igual forma, identifican en el sector empresarial una plataforma estratégica para lograr un mega-tejido, en prevención de delitos y cultura ciudadana.

Perspectiva España

Un buen referente para fundamentar la presente tendencia, lo ubicamos en el Código Penal Español, que integra no

solo la responsabilidad penal a las empresas, sino que advierte acerca de las bondades, de exigente de responsabilidad Código Penal Español (Art. 31 Bis No. 2) su función de supervisión, vigilancia y control (Art. 31 Bis No. 1-B) a través de las medidas que mitiguen la probabilidad de materialización del delito (Art. 31 Bis No. 2-1^a) a través de la supervisión del funcionamiento y del cumplimiento de un documento que marca las aristas más importantes que se deben proteger al que le denominan modelo de prevención penal (Art. 31 Bis No. 2-2^a).

Chile como referente suramericano

Al mismo tenor encontramos en el ordenamiento jurídico chileno, desde el 25 de noviembre del 2009, a través de la ley 20.393, la adopción de medidas que permiten integrar los compromisos adquiridos con la Organización para la Cooperación y Desarrollo Económico, OCDE, en la convención contra la corrupción, en el que se estipula la responsabilidad penal de las personas jurídicas en lo que respecta con los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho.

“Artículo 4°.- Modelo de prevención de los delitos. Para los efectos previstos en el inciso tercero del artículo anterior, las personas jurídicas podrán adoptar el modelo de prevención a que allí se hace referencia, el que deberá contener por lo menos los siguientes elementos:

- 1) Designación de un encargado de prevención
- 2) Definición de medios y facultades del encargado de prevención

- 3) Establecimiento de un sistema de prevención de los delitos
- 4) Supervisión y certificación del sistema de prevención de los delitos”.

Responsabilidad penal y deber de supervisión y control de las empresas en Colombia

Frente a una realidad ineludible en la que de manera global y de forma creciente, las legislaciones extranjeras prevén la posibilidad de extender la responsabilidad penal a las personas jurídicas (empresas), como instrumento de política criminal eficaz al estimular en las empresas la implementación de buenas prácticas de debida diligencia y mitigación de la probabilidad en la comisión de delitos; teniendo en cuenta que la delincuencia encuentra en la omisión de control y supervisión su mejor aliado para su materialización; que se encubre y mimetiza sigilosamente en el estado de desorden logístico empresarial, causando daño de niveles catastróficos y en ocasiones irreversibles a la continuidad del negocio; se puede afirmar que en materia de responsabilidad penal para las empresas (personas jurídicas) nuestra legislación interna adolece de mecanismos vinculantes, permaneciendo fiel a los tradicionales principios del antiguo y rígido axioma jurídico *“societas delinquere non potest”*, alocución latina que señala que las sociedades no pueden delinquir, por carecer de voluntad (elemento subjetivo) y por ende de capacidad de actuar con dolo (incapacidad de acción, culpabilidad y padecimiento de pena).

En este sentido, los tipos de autores y partícipes están expresos de manera taxativa en el Código Penal Colombiano, Ley 599 del 2000, que en sus artículos 28, 29 y 30 nuestro derecho se ciñe a un concepto restrictivo de autor; en el que el autor es el que realiza el tipo y los partícipes contribuirían a su realización, pero tiene en cuenta igualmente que autor es también quien realiza una parte de la ejecución de un plan conjunto (coautor) e incluso quien no realiza materialmente ningún hecho típico, pero controla la ejecución que es llevada a cabo por un instrumento al que utiliza (autor mediato).

En materia de las conductas derivadas del ejercicio empresarial, el Código Penal se vale de una cláusula de extensión de la autoría para aquellas personas físicas que actúan en lugar de las personas jurídicas (autor por representación), “quien actúa como miembro u órgano de representación autorizado o de hecho de una persona jurídica”, evidenciando marcada indiferencia con la responsabilidad penal directa de la persona jurídica.

No obstante a la renuente posición de extender la responsabilidad penal a las empresas, cabe resaltar sombras de tenue interés por admitir la importancia de la debida diligencia de supervisión y control de las personas jurídicas, como es el caso que evidencia el artículo 325 C.P., que eleva a conducta penal a la **omisión de control**, frente a una población empresarial determinada: “El empleado o director de una institución financiera o de cooperativas que ejerzan actividades de ahorro y crédito que, con el fin de ocultar o encubrir el origen ilícito

del dinero, omita el cumplimiento de alguno o todos los mecanismos de control establecidos por el ordenamiento jurídico para las transacciones en efectivo”.

De igual forma, es preciso advertir que, en materia penal, las empresas reciben su carga sancionatoria de conformidad con los mecanismos contemplados en la Ley 906 del 2004, que al respecto en su “Artículo 91. *Suspensión y cancelación de la personería jurídica*. En cualquier momento y antes de presentarse la acusación, a petición de la Fiscalía, el juez de control de garantías ordenará a la autoridad competente que, previo el cumplimiento de los requisitos legales establecidos para ello, proceda a la suspensión de la personería jurídica o al cierre temporal de los locales o establecimientos abiertos al público, de personas jurídicas o naturales, cuando existan motivos fundados que permitan inferir que se han dedicado total o parcialmente al desarrollo de actividades delictivas. Las anteriores medidas se dispondrán con carácter definitivo en la sentencia condenatoria cuando exista convencimiento más allá de toda duda razonable sobre las circunstancias que las originaron”. Lo antes expuesto, so pena del poder sancionatorio que otorgue el Estado a las autoridades administrativas que encausan y conminan el buen comportamiento empresarial en Colombia.

Intendente (Abogado)

HERNANDO ROJAS BALAGUERA

Gestor de Seguridad Empresarial
(Vinculación Empresas FESEM-DIJIN)

1.3 Identificación de los tipos penales que afectan la continuación del negocio en Colombia y medidas de control (Ley 599 de 2000)



"El conocimiento del riesgo criminal, le permite al empresario, prevenir".



<http://mimglobalservices.com/page14.php>

El Frente de Seguridad Empresarial como mecanismo de prevención criminal se permite entregar al empresario colombiano, el resultado de un trabajo de identificación de las conductas penales que pueden victimizarlo, con el fin de promover la apropiación de una cultura de seguridad que fomente y fortalezca la adopción de medidas en pro de su debida diligencia de supervisión y control; para mitigar la probabilidad de un delito que amenace su continuidad de negocio.

En este sentido, a continuación encontrará una matriz de tratamiento del delito como riesgo empresarial, que identifica **79 tipos penales**, luego de una revisión integral del Código Penal Colombiano y desde la experiencia de conocimiento del ejercicio de la investigación criminal registrada y subjetiva, organizada en forma alfabética para facilitar su comprensión, señalando el artículo que la contiene y las normas conexas en los casos que corresponden, las modalidades más recurrentes identificadas por personal cualificado de cada especialidad de la Policía Nacional, para al final emitir las recomendaciones y/o buenas prácticas empresariales en procura de trasladar a su mínima expresión la posibilidad de impacto en las diferentes actividades del quehacer empresarial, con presencia de negocio en Colombia.

Abuso de confianza**Ley 599 del 2000 C.P y otras normas sancionatorias:**

Art. 249

Tipología / modalidad delictiva:

- Apoderamiento indebido de cosa prestada, o alquilada.
- Disposición indebida de dineros dados en confianza por el empleador.

Procesos más vulnerables:

Administrativos
Operativos

Medidas de mitigación y continuidad de negocio:

- Estudios de seguridad en admisión y mantenimiento de personal.
- Entrenamiento fidelidad y sensibilización del talento humano.
- Auditorías cruzadas.
- Cultura de gestión y control interno.
- Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN.

Acaparamiento**Ley 599 del 2000 C.P y otras normas sancionatorias:**

Art. 297

Tipología / modalidad delictiva:

- Sustracción del comercio de artículo o producto de primera necesidad.

Procesos más vulnerables:

Directivos
Administrativos
Operativos

Medidas de mitigación y continuidad de negocio:

- Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal.
- Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal.
- Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal.
- Para el caso de los fabricantes y distribuidores, implementar controles que limiten el acceso con propósitos de acaparamiento del producto.
- Sujeción de su negocio al cumplimiento de los parámetros establecidos por la Ley 1480 2011 Estatuto del consumidor.

Apoderamiento de hidrocarburos, sus derivados, biocombustibles o mezclas que los contengan**Ley 599 del 2000 C.P y otras normas sancionatorias:**

Art. 327A CP
Ley 1028 de 2006

Tipología / modalidad delictiva:

- Extracción con válvula en poliducto
- Destinación ilegal (327D CP)

Procesos más vulnerables:

Administrativos
Operativos

Medidas de mitigación y continuidad de negocio:

- Fijación de estaciones de servicio legal y confiable para la provisión de combustibles.
- Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN.

Aceso abusivo a un sistema informático.	
Ley 599 del 2000 C.P y otras normas sancionatorias:	195/269A (CP) Ley 1273 de 2009
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Defacement (modificación de páginas Web) • APT (ataques persistentes a través de phishing o correos dirigidos -enlaces o archivos fraudulentos para robar información). • Keylogger (Captura de información pulsaciones del teclado). • DDoS (denegación de servicios). • Malware (Programa informático que ejecuta acciones ilegítimas). • Pharming (manipulación de archivos mediante el empleo de código malicioso). • Skimming (Clonación tarjetas). 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas de seguridad en la información (manejo de contraseñas, asignación de dominios individuales, actas de confidencialidad, apagado de equipo, clasificación de información, informe oportuno de novedades, guardado bajo llave de documentos impresos, escritorios y pantallas limpias, uso exclusivo de equipos de la empresa, controles de seguridad de instalaciones, no prestar usuarios, etc.). • Entrenamiento prevención delitos informáticos y seguridad de la información. • Designación de responsable y campañas en protección de datos. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Actualización antivirus y FireWire. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Agiotaje	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 301
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • En productos de primera necesidad • En materias primas • En salarios 	
Procesos más vulnerables:	Directivos Administrativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. • Sujeción de su negocio al cumplimiento de los parámetros establecidos por la Ley 1480 2011 Estatuto del consumidor. 	

Alteración y modificación de calidad, cantidad, peso o medida**Ley 599 del 2000 C.P y otras normas sancionatorias:** Art. 229**Tipología / modalidad delictiva:**

Alteración en perjuicio del consumidor

- La cantidad
- La calidad
- El peso

Procesos más vulnerables: Administrativos
Operativos**Medidas de mitigación y continuidad de negocio:**

- Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal.
- Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal.
- Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal.
- Procedimientos de adquisición, mantenimiento, control de calidad, calibración de equipos y materias primas.
- Sujeción de su negocio al cumplimiento de los parámetros establecidos por la Ley 1480 2011 Estatuto del consumidor.

Captación masiva y habitual de dineros**Ley 599 del 2000 C.P y otras normas sancionatorias:** Art. 316**Tipología / modalidad delictiva:**

• Captar dinero del público en forma masiva y habitual sin contar con la previa autorización. (Pirámides, cadenas, multinivel)

Procesos más vulnerables: Directivos
Administrativos
Operativos**Medidas de mitigación y continuidad de negocio:**

- Inclusión de prohibición de estas prácticas en el reglamento interno, fijando mecanismos de control que garantice su cumplimiento.
- Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal.

Circulación y uso de efecto oficial o sello falsificado**Ley 599 del 2000 C.P y otras normas sancionatorias:** Art. 281**Tipología / modalidad delictiva:**

• Haga circular sin haber falsificado. (Licencias, certificaciones, habilitaciones, permisos, paz y salvos, constancias, estampillas, entre otros)

Procesos más vulnerables: Directivos
Administrativos**Medidas de mitigación y continuidad de negocio:**

- Control y monitoreo a cumplimientos legales y supervisión de entidades públicas.
- Cultura de transparencia en participación de licitaciones.
- Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN.

Cohecho por dar u ofrecer	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 407
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Connivencia empresarial. • A título individual. 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Política de transparencia y cero tolerancia con la delincuencia. • Entrenamiento y sensibilización a empleados, consecuencias jurídicas. • No hacer mal uso de la posición dominante sobre el empleado. • La posición de reverencia y subordinación del empleado hacia el empleador no le exime de responsabilidad penal. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Concierto para delinquir	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 340
Tipología / modalidad delictiva:	
Confabulación para delinquir <ul style="list-style-type: none"> • Fuentes internas • Fuentes externas 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Política de transparencia y cero tolerancia con la delincuencia. • Entrenamiento y sensibilización a empleados, consecuencias jurídicas. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. • Estudios de confiabilidad en admisión y mantenimiento dirigido a los empleados. • Monitoreo temprano de potenciales concertaciones en grupo para afectar la empresa mediante infidelidad colectiva. • Control en la delegación de funciones (evitar concentración de poder y excesos de confianza en los empleados) 	

Contaminación ambiental culposa por explotación de yacimiento minero o hidrocarburo

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 333
Tipología / modalidad delictiva:		
<ul style="list-style-type: none"> • En exploración • En explotación • En extracción 		
Procesos más vulnerables:		Administrativos Operativos
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Adopción de buenas prácticas ambientales. • Cumplimiento normatividad vigente en la materia. (Ley 685 de 2001 Código de Minas, Ley 1382 2009, Ley 1333 2009 procedimiento sancionatorio ambiental, Ley 1252 del 2008 normas prohibitivas en materia ambiental, referentes a los residuos y desechos peligrosos) • Expedición licencias ambientales (ANLA). • Plan de simulacros y contingencias. <p style="text-align: right;">• Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN.</p>		

Contaminación ambiental por residuos sólidos peligrosos

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 332A
Tipología / modalidad delictiva:		
<ul style="list-style-type: none"> • Inadecuada disposición de escombros y demás residuos sólidos industriales. 		
Procesos más vulnerables:		Operativos
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Control de residuos sólidos y destinación final. • Manejo legal de disposición residuos. • Aplique la regla de las 3 R de la ecología en la empresa (reduzca, reutilice y recicle). • Sensibilice en su personal la importancia de la Ley 99 de 1993 Sistema Nacional Ambiental, SINA. • Implementación ISO 14001. (Sistema de Gestión Ambiental) • Prevención de contaminación. Control de los impactos ambientales, Cumplimiento legislación, Mejoramiento continuo. 		

13

33

Contaminación ambiental	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 332
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Al aire • A la atmósfera • Al espacio aéreo • Al suelo • Al subsuelo • El agua 	
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Sensibilice en su personal de la importancia de la Ley 99 de 1993 Sistema Nacional Ambiental, SINA. • Política de desarrollo sostenible: sujeción del crecimiento económico, a la elevación de la calidad de la vida y al bienestar social, sin agotar la base de recursos naturales renovables. • Implementación ISO 14001. (Sistema de Gestión Ambiental) • Prevención de contaminación. Control de los impactos ambientales, Cumplimiento legislación, Mejoramiento continuo. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

14

Contaminación de aguas	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 371
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Destinada al consumo humano 	
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Control de residuos y su destinación final. • Sensibilice en su personal la importancia de la Ley 99 de 1993 Sistema Nacional Ambiental SINA. • Implementación ISO 14001. (Sistema de Gestión Ambiental) • Prevención de contaminación. Control de los impactos ambientales, Cumplimiento legislación, Mejoramiento continuo. • Prevenir impactos ambientales en el manejo de sustancias químicas. • Capacitación, entrenamiento y sensibilización ambiental del personal. • Control de vertimientos de sus instalaciones. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Contrabando de hidrocarburos y sus derivados	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Decreto 1900 de 2002, Decreto 2180 de 2002
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Abierto • Técnico • Desviación de destino • Tanques y caletas camuflados (en paso de frontera) 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas claras con los conductores. • Entrenamiento sensibilización de la modalidad delictiva y sus consecuencias penales, administrativas y traumatismo logístico a la operación. • Clausulado contractual que penalice este riesgo. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Contrabando	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 319 CP Ley 1762 de 2015
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Abierto • Técnico 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas claras con los empleados. • Entrenamiento sensibilización de la modalidad delictiva y sus consecuencias penales, administrativas y traumatismo logístico a la operación. • Clausulado contractual que penalice este riesgo. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Daño en bien ajeno	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 265
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Sobre bienes de particulares. • Sobre bienes del Estado 	
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas de buen uso de bienes propios y respeto por los de terceros. • Protocolos de seguridad industrial y de procesos seguros. • Promoción al deber objetivo de cuidado. • Entrenamiento sensibilización de la modalidad delictiva y sus consecuencias penales. 	

18

35

Daño Informático	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 269D
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Malware (Programa informático que ejecuta acciones ilegítimas y desautorizadas). • APT (ataques persistentes avanzados a través de phishing o correos dirigidos para obligar a un usuario para que ingrese a enlaces o archivos fraudulentos). 	
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas de seguridad en la información (manejo de contraseñas, asignación de dominios individuales, actas de confidencialidad, apagado de equipo, clasificación de información, informe oportuno de novedades, guardado bajo llave de documentos impresos, escritorios y pantallas limpias, uso exclusivo de equipos de la empresa, controles de seguridad de instalaciones, no prestar usuarios, etc.). • Designación de responsable y campañas en protección de datos. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Actualización antivirus y FireWire. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. • Implementación ISO 27001. 	

19

Defraudación a las rentas de aduana	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 321
Tipología / modalidad delictiva:	
Declaración de tributos aduaneros por un valor inferior al que por ley le corresponde.	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Entrenamiento y sensibilización a empleados, consecuencias jurídicas. • No hacer mal uso de la posición dominante sobre el empleado. • La posición de reverencia y subordinación del empleado hacia el empleador no le exime de responsabilidad penal. • Trámites aduaneros con agentes autorizados y reconocidos. • Políticas de transparencia administrativa. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Defraudación a los derechos patrimoniales de autor	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 271
Tipología / modalidad delictiva:	
En obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador.	
Procesos más vulnerables:	Directivos Administrativos
Medidas de mitigación y continuidad de negocio:	
<p>Cumplir con las obligaciones de recaudo con las sociedades de gestión colectiva, por comunicación pública de obras protegidas cuando a ello haya lugar. SAYCO (Sociedad de Autores y Compositores de Colombia), ACINPRO (Asociación Colombiana de Intérpretes Productores Fonográficos), ACODEM (Asociación Colombiana de Editores de Música), APDIF (Asociación para la Protección de los Derechos Intelectuales Fonogramas Musicales), CDR (Centro Colombiano de Derechos Reprográficos), MPLC (Motion Picture Licensing Corporation).</p> <ul style="list-style-type: none"> • Actualización de licenciamientos. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Del tráfico de personas y tráfico de migrantes	
Ley 599 del 2000 C.P y otras normas sancionatorias:	180 CP Ley 747 de 2002 Ley 985 de 2005
Tipología / modalidad delictiva:	
Por Lucro u otro provecho para sí u otra persona. Explotación por prostitución, pornografía, servidumbre por deudas, mendicidad, trabajo forzado	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Programas de sensibilización de los peligros de la migración internacional realizada bajo condiciones de vulnerabilidad, riesgo, irregularidad o ilegalidad. • Formalidad y cumplimiento de obligaciones en materia laboral. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Desaparición forzada	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 165
Tipología / modalidad delictiva:	
Someter a otra persona a privación de su libertad cualquiera que sea la forma, seguida de su ocultamiento y de la negativa a reconocer dicha privación o de dar información sobre su paradero	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Diagnóstico y tratamiento de riesgo personal a los funcionarios que por su posición económica, de representatividad, exposición en zonas críticas y vulnerabilidad estén expuestas a posibles retaliaciones de grupos ilegales. • Políticas de autocuidado y autoprotección. • Control de rutinas, panorámicas de riesgo. • Comunicaciones efectivas con las autoridades en especial DIASE. • Control de ubicación y desplazamiento de los empleados. 	

Destinación ilícita de muebles o inmuebles	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 377
Tipología / modalidad delictiva:	
Destinar ilícitamente bien mueble o inmueble para que en él se elabore, almacene o transporte, venda o use sustancias estupefacientes.	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Ejercer el deber objetivo de cuidado y supervisión sobre los bienes inmuebles de la empresa y el uso que se le está dando. • Realizar visitas impredecibles y aleatorias a los inmuebles de la empresa. • Abstenerse de tener inmuebles en estado de abandono o avanzado deterioro, faltos de vigilancia o entregados en custodia en confianza excesiva. • Debida diligencia y cuidado como titular del bien. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. • Estos bienes inmuebles pueden ser objeto de extinción de dominio y revisten responsabilidad penal sobre el titular. 	

Emisión y transferencia ilegal de cheque

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 248
Tipología / modalidad delictiva:		
Fraude mediante cheque		
Procesos más vulnerables:		Directivos Administrativos
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. • Procedimientos de control y monitoreo de activos (estados financieros). • Estudio de procedencia de clientes y activos relacionados. Políticas de control interno. • Control en la delegación de funciones (evitar concentración de poder y excesos de confianza en los empleados) • Estudios de confiabilidad en cargos de confianza y manejo. 		

Enriquecimiento ilícito de particulares

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 327
Tipología / modalidad delictiva:		
Incremento patrimonial no justificado, derivado de actividades delictivas		
Procesos más vulnerables:		Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. • Procedimientos de control y monitoreo de activos (estados financieros). • Estudio de procedencia de clientes y activos relacionados. Políticas de control interno. • Control en la delegación de funciones (evitar concentración de poder y excesos de confianza en los empleados) • Estudios de confiabilidad a cargos de confianza y manejo. 		

Especulación	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 298
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Fábrica o distribución artículo o género de primera necesidad a precios superiores. 	
Procesos más vulnerables:	Directivos Administrativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. • Procedimientos de control y monitoreo de precios regulados. • Adopción de políticas de corresponsabilidad penal. • Sujeción de su negocio al cumplimiento de los parámetros establecidos por la Ley 1480 2011, Estatuto del consumidor. 	

Estafa	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 246
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Llamada millonaria-tio/tia-ahorros programados viajes. • Falso abogado. • Estafa carcelaria. • Suplantación de empresa (utilización de su buen nombre, para la apropiación ilegal de mercancías y dineros). • Falso proponente en licitación pública, para apropiación ilegal de anticipos. • Falso alquiler de vehículos, a nombre de empresas reconocidas. • Captación ilegal de recursos para la construcción de falsos proyectos. • Falsa oferta de empleo para aplicar en las diferentes vacantes de empresas de alto reconocimiento. • Defraudación mediante ofrecimiento de falsos títulos valores. • Venta ilegal de predios e inmuebles con datos y documentación falsa. • Representante de falsa fundación. • Falsa evidencia para sobrefacturar prestación de servicios. <p>Realización de trámites, mediante datos y documentos falsos.</p>	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Implementación de protocolos que eviten la rutina, automatización de respuestas y mecanización de procedimientos. • Políticas y protocolos claros y seguros para autorizar desembolsos. • Trazabilidad de procedimientos que facilite futuras investigaciones y verificaciones.. • El tamaño de la empresa no determina el grado de vulnerabilidad, todas están expuestas. • Capacitación y sensibilización de las consecuencias penales administrativas y dirigido especialmente a los cargos de manejo y confianza. • Política de legalidad y cero tolerancia con la delincuencia liderada por socios y nivel directivo. • Sospecha de clientes con ofertas inusuales o que ofrezcan marcada ventaja comercial. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Explotación ilícita de yacimiento minero y otros materiales	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 338
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Extracción ilegal de minerales (con incidencia grupo armado ilegal) • Extracción ilegal de minerales (como fenómeno social) 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Adopción de buenas prácticas ambientales. • Cumplimiento normatividad vigente en la materia. (Ley 685 de 2001 Código de Minas, Ley 1382 2009, Ley 1333 2009 procedimiento sancionatorio ambiental, Ley 1252 del 2008 normas prohibitivas en materia ambiental, referentes a los residuos y desechos peligrosos). • Expedición de licencias ambientales (ANLA). • Denunciar los sitios afectados por el fenómeno a la Dirección de Carabineros. • Evitar vínculo de negocio que fomente esta actividad ilegal. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Exportación o importación ficticia	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 310
Tipología / modalidad delictiva:	
Simulación, exportación o importación.	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Política de legalidad y cero tolerancia con la delincuencia. • Gestión de Control interno. • Utilización de agentes y canales de intermediación autorizados por la DIAN. • Sensibilización interna de las consecuencias penales, de continuidad de negocios y reputaciones de la conducta punible. • Manejo de la guía de control de riesgos financieros (ONU NRS). • Adopción política conozca su cliente. • Implementación de modelos de mitigación de riesgos LA/FT. (OEA, SIPLAF, BASC etc.). • Control en la delegación de funciones (evitar concentración de poder y excesos de confianza en los empleados). • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Extorsión	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 244
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Carcelaria (A través de internos en centros penitenciarios realizan llamadas a las víctimas) • Clásica (Por lo general los victimarios son cercanos al núcleo familiar o laboral de su víctima) • Menor cuantía (Exigen pequeñas sumas de dinero en forma reiterada y persistente). 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Diagnóstico y tratamiento de riesgo personal a los funcionarios que por su posición económica, de representatividad, exposición en zonas críticas y vulnerabilidad estén expuestas a posibles retaliaciones de grupos ilegales. • Estudios de seguridad al Personal en pre-empleo, rutina y específicos. • Diagnóstico y tratamiento de riesgo personal a los funcionarios que por su posición económica, de representatividad, exposición en zonas críticas y vulnerabilidad estén expuestas a extorsión. • Designación de responsable y campañas en protección de datos. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Evite excesos de confianza, rutinas, transportar cuantiosas cifras de dinero, actitudes suntuosas, exposición de información privada. 	

Fabricación, tráfico y porte de armas de fuego o municiones	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 365 CP Art. 223 Constitución Política, Monopolio estatal. Decreto 2535/93 normas sobre Armas, Municiones y Explosivos
Tipología / modalidad delictiva:	
Importación ilegal <ul style="list-style-type: none"> • Armas (Introducción clandestina al país y camufladas en mercancías) • Partes (revueltas con repuestos y camufladas en otras mercancías) Mercado Negro <ul style="list-style-type: none"> • Armas hurtadas, perdidas y alquiladas ilegalmente. 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Implementación de procesos que garanticen la trazabilidad y no contaminación de la carga importada. • Procesos de seguimiento a cargos sensibles, desconcentración de poder en funcionarios, pruebas de confiabilidad periódica. • Ejercicio ético y responsable de negocios. • Implementar estrictos protocolos para el transporte y custodia de armas. • Política de cero tolerancia con la delincuencia. • Complementos tecnológicos de rastreo satelital a guardas y armas (geo cercas) • Cumplimiento lineamientos y leyes vigentes. 	

Falsa denuncia**Ley 599 del 2000 C.P y otras normas sancionatorias:**

Art. 435, Art. 436

Tipología / modalidad delictiva:

- Conducta típica que no se ha cometido.
- Contra persona como autor o partícipe de una conducta típica que no ha cometido

Procesos más vulnerables:

Directivos
Administrativos
Operativos

Medidas de mitigación y continuidad de negocio:

- Adopción de negocios responsables éticos y legales.
- No contestar con la denuncia como mera formalidad de trámite para reclamación de pólizas de seguro.
- No inculpar soportados en supuestos o sospechas infundadas.
- Designar la responsabilidad de denuncia al Representante Legal o Judicial con criterio y seriedad.
- Una vez denunciado el hecho punible acompañe y colabore el proceso investigativo.

Falsedad en documento privado**Ley 599 del 2000 C.P y otras normas sancionatorias:**

Art. 289

Tipología / modalidad delictiva:

Usos para trámites comerciales (entidades privadas), entidades y trámites públicos.

Procesos más vulnerables:

Directivos
Administrativos
Operativos

Medidas de mitigación y continuidad de negocio:

- No descuidar sus documentos de identidad, tanto públicos como privados (Cédulas, carnet, documentos de tránsito, etc.).
- No prestar ni depositar en confianza (familia, cónyuge, amigos etc.) los documentos de identidad personal de ninguna índole.
- Implementación de proceso de asignación, control y destrucción de carnets de la compañía.
- Garantizar la trazabilidad y manejo de documentos mediante el registro documentado.
- Control de papelería membretada.
- Fortalecimiento del personal en principios básicos para la detección temprana de documentos falsos.
- Adopción de medidas de disuasión y sensibilización que fortalezca la fidelización y lealtad del personal.

34

43

Falsedad marcaría	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 285
Tipología / modalidad delictiva:	
Sobre marca, contraseña, signo, firma o rúbrica usados oficialmente para contrastar, identificar o certificar peso, medida, calidad, cantidad, valor o contenido.	
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. • Para el caso de los fabricantes y distribuidores implementar controles de calibración y controles de calidad, pesos y medidas. • Sujeción de su negocio al cumplimiento de los parámetros establecidos por la Ley 1480 2011, Estatuto del consumidor. 	

35

Falsedad material en documento público	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 287
Tipología / modalidad delictiva:	
Usos para trámites comerciales (entidades privadas), entidades y trámites públicos.	
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • No descuidar sus documentos de identidad, tanto públicos como privados (Cédulas, documentos de tránsito, etc.). • No prestar ni depositar en confianza (familia, cónyuge, amigos etc.) los documentos de identidad personal de ninguna índole. • Garantizar la trazabilidad y manejo de documentos mediante el registro documentado. • Fortalecimiento de competencias al personal en principios básicos para la detección temprana de documentos falsos. • Adopción de medidas de disuasión y sensibilización que fortalezca la fidelización y lealtad del personal. 	

Falsedad personal

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 296
Tipología / modalidad delictiva:		
Sustituya o suplante a una persona (Cédula, Tarjeta de Identidad, Registro Civil nacido vivo, etc.).		
Procesos más vulnerables:	Directivos Administrativos Operativos	
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Especial cuidado y mantenimiento con sus documentos de identidad. • Fortalecimiento en competencias al personal en principios básicos para la detección temprana de documentos falsos. • Implementar y respetar la Ley 1581 del 2012, Habeas Data. • Manejo políticas de confidencialidad a la información del personal y clientes administrada en el ejercicio del negocio correspondiente. 		

Falsificación de efecto oficial timbrado

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 280
Tipología / modalidad delictiva:		
Falsifique estampilla oficial		
Procesos más vulnerables:	Administrativos Operativos	
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. • Para el caso de objetos de negocios obligados a contribuciones especiales dar oportuno cumplimiento. • Sujeción de su negocio al cumplimiento arbitrio rentístico. 		

Falsificación o uso fraudulento de sello oficial

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 279
Tipología / modalidad delictiva:		
Falsificación de sello oficial o uso fraudulento.		
Procesos más vulnerables:	Administrativos Operativos	
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. • Sujeción de su negocio al cumplimiento de formalidad impuesta por entidades públicas. 		

Favorecimiento de contrabando

Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 320 CP Ley 1762 de 2015
Tipología / modalidad delictiva:	
Introducir al territorio colombiano mercancías por lugares no habilitados, u ocultada, disimulada o sustraída de la intervención y control aduanero.	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas claras con los empleados. • Entrenamiento sensibilización de la modalidad delictiva y sus consecuencias penales, administrativas y traumatismo logístico a la operación. • Clausulado contractual que penalice este riesgo. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. • Intermediación aduanera legal y mediante compañías confiables. 	

Financiación del Terrorismo

Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 345 CP Ley 1121 de 2006
Tipología / modalidad delictiva:	
Directa o indirectamente 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.	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. • Estudios de seguridad al personal en preempleo, rutina y específicos. • Diagnóstico y tratamiento de riesgo personal a los funcionarios que por su exposición en zonas críticas y vulnerabilidad estén expuestas a este delito. • Políticas de autocuidado y autoprotección. • Comunicaciones efectivas con las autoridades. • Política "Yo no pago, yo denuncio". • Designación de responsable oficial cumplimiento ante UIAF. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Evite excesos de confianza, rutinas, transportar cuantiosas cifras de dinero, actitudes suntuosas, exposición de información privada. 	

Hurto por medios informáticos y semejantes

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 269 I
Tipología / modalidad delictiva:		
<ul style="list-style-type: none"> • Ingeniería social (práctica social de obtener información a través del engaño) • Phishing (suplantación de sitios Web para capturar datos personales de la víctima) • Malware (Programa informático que ejecuta acciones ilegítimas y desautorizadas en un sistema informático) • Skimming (Conducta que consiste en la clonación de tarjetas débito y crédito) • Suplantación de identidad (empleo de la información personal de un tercero para obtener de manera ilegítima recursos o beneficios propios de la víctima) • Vishing (ingeniería social llevada a cabo mediante llamadas telefónicas) 		
Procesos más vulnerables:		Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Políticas de seguridad en la información (manejo de contraseñas, asignación de dominios individuales, actas de confidencialidad, apagado de equipo, clasificación de información, informe oportuno de novedades, guardado bajo llave de documentos impresos, escritorios y pantallas limpias, uso exclusivo de equipos de la empresa, controles de seguridad de instalaciones, no prestar usuarios, etc.). • Entrenamiento prevención de delitos informáticos y seguridad de la información. • Designación de responsable y campañas en protección de datos. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Actualización antivirus y FireWire. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 		

Ilícito aprovechamiento de los recursos naturales renovables

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 328
Tipología / modalidad delictiva:		
<ul style="list-style-type: none"> • Sobre fauna • Sobre recurso hidrobiológicos (En especies amenazadas o en vía de extinción).		<ul style="list-style-type: none"> • Sobre flora
Procesos más vulnerables:		Administrativos Operativos
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Cumplimiento de la normatividad existente para el aprovechamiento de especies y recursos renovables. • Ejercer la actividad industrial bajo políticas de responsabilidad social, desarrollo sostenible. • Retribuir y restaurar los impactos ambientales a la Fauna y Flora, causada por el ejercicio de su negocio. 		

Hurto en la cadena de suministro	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 239
Tipología / modalidad delictiva:	
<p>Mercancías en la Cadena del Suministro (Piratería Terrestre)</p> <ul style="list-style-type: none"> • Atraco (uso de armas, sometimiento por la fuerza) • Autohurto (Con complicidad y/o connivencia de funcionarios de la empresa) • Gemeleo (mediante vehículo acondicionado con características y placa de otro). • Saqueo de contenedores (Hurto parcial mediante violación de cerraduras, o remoción de bisagras -Parqueaderos y puertos-) • Suplantación de autoridad (Falsos puestos de control policial) • Suplantación de identidad (valiéndose de falsedad personal) • Uso de sustancias psicoactivas (induciendo trastorno mental y manipulación de la voluntad) • Descuelgue (hurto parcial con escalonamiento al vehículo, en lugares de tránsito lento o parada) Repartidores TAT (Hurto contra las cadenas de distribución tienda a tienda) 	
Procesos más vulnerables:	<p>Administrativos</p> <p>Operativos</p>
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Análisis y tratamiento de riesgo por criticidad de mercancías y zonas de mayor afectación. • Designación de Jefe de Seguridad, responsable de control y monitoreo de tráfico con competencias de idoneidad específicas. • Estudio de seguridad de asociados de negocio. • Implementación de plataforma tecnológica para fidelización de conductores. • Estudio de seguridad a conductores y propietarios de vehículos de carga mediante acuerdos de seguridad que involucre verificación de identidad, antecedentes, visitas domiciliarias e intercambio de información y record de cumplimientos con otras empresas del gremio. • Política de monitoreo satelital a todo vehículo antes de ser despachado. • Sistemas de puestos fijos de control y seguimiento. • Monitoreo telefónico a conductores. • Activa participación y vinculación con el Frente de Seguridad Empresarial y RISTRA de la Policía Nacional. • Estudios de seguridad para seguimiento a personal interno que ostente cargo sensible (acceso a información y activos). • Evitar concentración de poder y confianza excesiva en empleados. • No pagar comisiones a tramitadores e intermediarios. • Fijar condiciones y estabilidad laboral a sus empleados. • Integrar sistemas de comunicación grupal que facilite el acceso a información útil a la seguridad en tiempo real. • Fijar criterios que garanticen una adecuada selección de proveedor de monitoreo satelital. • Políticas de fijación y selección de escoltas. • Implementación de procesos trazables. • Capacitación y sensibilización permanente al personal de la empresa y conductores tercerizados. • Accesibilidad de información que permita orientar a las autoridades en caso de siniestro. • Notificación de condición plan de ruta (hoteles, parqueaderos, ruta, restaurantes, estaciones de servicio autorizados) 	

Hurto (Comercio)

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 239
Tipología / modalidad delictiva:		
Comercio		
<ul style="list-style-type: none"> • Atraco (uso de fuerza, armas de fuego) • Hormigueo (Mercancías Hurtadas desde los puntos de venta al público) • Falsa diligencia de Policía Judicial. 		
Procesos más vulnerables:		Administrativos Operativos
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Adopción de procedimientos y desarrollos tecnológicos que garanticen un fidedigno control de inventarios. • Implementación de circuito cerrado de televisión con designación de funcionarios idóneos en su monitoreo. • Establecimiento de criterios para la selección adecuada de empresas de vigilancia y seguridad privada, que obedezcan a un diagnóstico de necesidades previas. • Trabajo articulado con las autoridades, colaboración y suministro de información. • Escenarios de retroalimentación de información con pares de negocio. • Actividad de vigilancia mediante cliente encubierto. • Entrenamiento periódico dirigido a los empleados disuasión y desestímulo a infidelidades. • Disponer de lockers a la entrada para evitar que los clientes entren con bolsos. • Control especial a personas de actitud sospechosa, vestimenta suelta, coches, bebes de brazos o que aborden en grupo a un solo vendedor. • Manejo de sistemas de código de barras, pines, antenas y demás tecnología de sistema anti-hurto. • Sistemas de pánicos, alarmas y comunicación eficiente con la patrulla del cuadrante. • Seguimiento, análisis y colaboración postdenuncia a las investigaciones penales que se deriven de flagrancias. • Monitoreo y reporte temprano de situaciones sospechosas del entorno público, parqueaderos y zonas comunes de las instalaciones. 		

Obstrucción a vías públicas que afecten el orden público

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 353A CP 2011 Art. 44	Ley 1453
Tipología / modalidad delictiva:			
Incitar, dirigir, constreñir o proporcionar los medios			
Procesos más vulnerables:		Administrativos Operativos	
Medidas de mitigación y continuidad de negocio:			
<ul style="list-style-type: none"> • Cultura de gestión y control interno. 			

Hurto de Automotores**Ley 599 del 2000 C.P y otras normas sancionatorias:**

Art. 239

Tipología / modalidad delictiva:

Halado (aprovechamiento descuido)

- Utilización Ganzúas
- Violación de Guardas
- Ruptura de Vidrios
- Copia de la llave

Atraco

- Simulación accidente
- Suplantación de autoridad
- Cierre en Semáforos
- Personas como señuelos
- Falsos puestos de control policial
- Empleo de Sustancias Tóxicas
- En semáforos
- En centros comerciales o lugares concurridos
- Bares y discotecas
- Hurto con Cobro Extorsivo
- Seguimiento a la víctima - Hurto del vehículo - ubicación de la víctima -Exigencia económica.
- Autorrobo
- Venta en frontera
- Venta con documentación falsa
- Venta para cobro de seguro
- Doble aseguramiento
- Pago de extorsiones
- Denuncia ficticia

Procesos más vulnerables:

Directivos
Administrativos
Operativos

Medidas de mitigación y continuidad de negocio:

- Gestión del riesgo conforme a criticidad por vulnerabilidad de marcas del parque automotor.
- Plan de sensibilización y capacitación recomendaciones para prevenir el hurto de vehículos.
- Cultura de disciplina y cumplimiento de protocolos de seguridad con los vehículos (parqueaderos autorizados, rutas programadas, reporte telefónico, control de tráfico, monitoreo satelital, precisión contractual con propietarios y conductores, manejo de pólizas, estudios de seguridad y confiabilidad de conductores etc.)
- Relacionamiento y comunicación efectiva con las autoridades.
- Cero tolerancia con la delincuencia (no a pago de extorsiones)
- No exponerse en lugares de nivel de riesgo o altas horas de la noche.
- Control y verificación de horarios de parqueo de vehículos.
- No dejar abandonado el vehículo.
- Aviso oportuno de amenazas.
- Tenga instalado la aplicación POLIS (sincronizar su celular con el celular del cuadrante correspondiente a su ubicación).

Hurto. (Personas -Residencias)**Ley 599 del 2000 C.P y otras normas sancionatorias:**

Art. 239

Tipología / modalidad delictiva:

Personas

- Atraco (uso de fuerza y armas)
- Fleteo (Víctima que retira dinero del sistema bancario)
- Cosquilleo (Aprovechamiento de tumultos)
- Paseo Millonario (complicidad de conductores de servicio público)
- Rasponazo (Oportunidad y huida)

Residencias/ Instalaciones

- Ventosa (hueco en la pared)
- Falso visitante (falso interés de tomar arriendos o compras de inmueble)
- Falso allanamiento(Suplantan Policía Judicial)
- Suplantación de empleados de servicios públicos.
- Penetración (Fuga de información por empleado/a que labora dentro de la residencia)
- Mal vecino (toman en arriendo contigo al de la víctima, para acceder a información)

Procesos más vulnerables:

Administrativos
Operativos

Medidas de mitigación y continuidad de negocio:

- Adopción de cultura de manejo mínimo de efectivo (tarjetas débito y crédito, cheques, transacciones electrónicas, etc.).
- Manejo de confidencialidad de operaciones financieras.
- Adopte medidas de seguridad en retiros en efectivo (acompañamiento policial, observación entorno bancario, personas sospechosas dentro del banco, etc.).
- Tenga instalado la aplicación POLIS (sincronizar su celular con el celular del cuadrante correspondiente a su ubicación).
- Frente a la inevitable necesidad de transportar efectivo distribúyalo en varias partes.
- Evite utilizar públicamente accesorios y lujos de alto valor (joyas, celulares, tablet).
- Refuerce y asegure las autopartes de fácil remoción.
- Asegure sus pertenencias al abordar un sistema de transporte masivo, o en sitios de alta concurrencia de personas.
- No divulgue las vulnerabilidades de sus instalaciones y/o residencia.
- Implemente estudio panorámico de seguridad física y mitigue el riesgo (seguridad humana, barreras perimetrales, controles de accesos, CCTV, sensores, control de inventarios, seguridad canina, control visitantes, control funcionarios, pruebas de vulnerabilidad, estudios de confiabilidad de personal, monitoreo de pérdidas y defraudaciones, acciones preventivas, disuasivas, campañas, etc.).
- Relaciónese y conozca el entorno vecindario (su seguridad trasciende las paredes de su instalación).
- Política de cero tolerancia corporativa con la delincuencia.

Intercepción de datos informáticos	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 269C
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Keylogger (Programa informático que captura la información por teclado) • Sniffer (Programa informático empleado por los delincuentes para interceptar comunicaciones) • Phishing (Es la suplantación de sitios Web para capturar datos personales de la víctima). • APT (Corresponde a los ataques persistentes avanzados a través de phishing o correos dirigidos para obligar a un usuario para que ingrese a enlaces o archivos fraudulentos). 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas de seguridad en la información (manejo de contraseñas, asignación de dominios individuales, actas de confidencialidad, apagado de equipo, clasificación de información, informe oportuno de novedades, guardado bajo llave de documentos impresos, escritorios y pantallas limpias, uso exclusivo de equipos de la empresa, controles de seguridad de instalaciones, no prestar usuarios, etc.). • Entrenamiento prevención de delitos informáticos y seguridad de la información. • Designación de responsable y campañas en protección de datos. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Asistencia a través de CAI virtual (Aplicación y servicio chat) • Actualización antivirus y FireWire. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Omisión de control	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 325
Tipología / modalidad delictiva:	
Omisiones por empleado o director de una institución financiera o de cooperativas, que con el fin de ocultar o encubrir el origen ilícito del dinero, omita el cumplimiento de alguno o todos los mecanismos de control establecidos por el ordenamiento jurídico.	
Procesos más vulnerables:	Directivo Administrativo
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Cumplir con las obligaciones de control y supervisión que exige la legislación vigente. • Seguimiento y prevención con requisitos SIPLAFT. • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. 	

Lavado de activos	
Ley 599 del 2000 C.P y otras normas sancionatorias:	
	Art. 323 (CP) modificado por Ley 1762 de 2015
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Fraccionamiento de dinero. • Tarjetas de crédito. • Giros Nacional e Internacional utilizando el nombre de la empresa • Exportaciones ficticias • Falso siniestro para afectar póliza. • Bitcoins (Moneda virtual). <li style="text-align: right;">• Operaciones off shore 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Estudios de seguridad asociados de negocio. • El tamaño de la empresa no determina el grado de vulnerabilidad, todas están expuestas. • Manejo de la guía de control de riesgos financieros (ONU NRS). • Adopción política, conozca su cliente. • Implementación de modelos de mitigación de riesgos LA/FT. (OEA, SIPLAF, BASC, etc.). • Designación de Oficial de Cumplimiento. • Control en la delegación de funciones (evitar concentración de poder y excesos de confianza en los empleados) • Estudio y monitoreo de estados financieros. • Acuerdos mutuos de seguridad. • Capacitación y sensibilización de las consecuencias penales administrativas y reputacionales dirigido especialmente a los cargos de manejo y confianza. • Política de legalidad y cero tolerancia con la delincuencia liderada por socios y nivel directivo. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Obstaculización ilegítima de sistema informático o red de telecomunicación	
Ley 599 del 2000 C.P y otras normas sancionatorias:	
	Art. 269B
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • DDoS (denegación de servicios que puede sufrir un sistema informático) • Malware (Programa informático que ejecuta acciones ilegítimas y desautorizadas en un sistema informático) • Ransomware/Cryptolocker (Programa informático empleado por los delincuentes para cifrar la información contenida en un computador y luego pedir recompensa) 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas de seguridad en la información • Entrenamiento prevención de delitos informáticos y seguridad de la información. • Designación de responsable y campañas en protección de datos. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Asistencia a través de CAI virtual (Aplicación y servicio chat) • Actualización antivirus y FireWire. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

52

53

Ofrecimiento engañoso de productos y servicios

Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 300
Tipología / modalidad delictiva:	
Ofrecer al público bienes o servicios en forma masiva, sin que los mismos correspondan a la calidad o características anunciadas.	
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. • Para el caso de los fabricantes y distribuidores implementar controles que garanticen la correspondencia del producto con la expectativa creada al consumidor. • Sujeción de su negocio al cumplimiento de los parámetros establecidos por la Ley 1480 2011, Estatuto del consumidor. 	

53

Omisión del agente retenedor o recaudador

Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 402
Tipología / modalidad delictiva:	
No consignar las sumas retenidas o autorretenidas por concepto de retención en la fuente. Impuesto sobre las ventas que, teniendo la obligación legal de hacerlo, no consigne las sumas recaudadas por dicho concepto	
Procesos más vulnerables:	
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Cumplir con las obligaciones tributarias que exige la legislación vigente. • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. 	

54

Operaciones no autorizadas con accionistas o asociados

Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 315
Tipología / modalidad delictiva:	
Favorecer ilegalmente a accionistas o asociados de la propia entidad financiera.	
Procesos más vulnerables:	Directivo Administrativo
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Cumplir con las obligaciones de control y supervisión que exige la legislación vigente. • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. 	

Pánico económico	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 302
Tipología / modalidad delictiva:	
Difusión de información falsa o inexacta que pueda afectar la confianza de los clientes, usuarios, inversionistas o accionistas de una entidad financiera.	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Sensibilización en todos los niveles de las consecuencias penales, sociales, administrativas que implica esta práctica ilegal. 	

Receptación	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 447
Tipología / modalidad delictiva:	
Adquirir, poseer, convertir o transferir bienes muebles o inmuebles, que tengan su origen mediato o inmediato en un delito	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Política de legalidad y cero tolerancia con actos delictivos. • Estudios de seguridad para seguimiento a personal interno que ostente cargo sensible (acceso a información y activos) • Evitar concentración de poder y confianza excesiva en empleados. • Adopción de procedimientos y desarrollos tecnológicos que garanticen un fidedigno control de inventarios. • Implementación de circuito cerrado de televisión con designación de funcionarios idóneos en su monitoreo. • Trabajo articulado con las autoridades, colaboración y suministro de información. • Escenarios de retroalimentación de información con pares de negocio. • Entrenamiento periódico dirigido a los empleados, disuasión y desestímulo a infidelidades. • Seguimiento, análisis y colaboración postdenuncia a las investigaciones penales que se deriven de flagrancias. • Entrenamiento y sensibilización a empleados, consecuencias jurídicas. • Proveedores de distribuidoras reconocidas y legalmente constituidos. 	

Sabotaje.	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 199
Tipología / modalidad delictiva:	
Daños para suspender o paralizar el trabajo sobre: <ul style="list-style-type: none"> • Bases de datos • Instalaciones • Materias primas 	<ul style="list-style-type: none"> • Herramientas • Soportes lógicos • Equipos
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Estudios de selección y mantenimiento de personal. • Sensibilización para fortalecer lealtad y fidelización. • Cumplimiento oportuno y legal de las obligaciones laborales. • Clasificación y señalización de ingresos no autorizados. • Capacitación de consecuencias penales y traumatismo logística del delito. • Planes de continuidad de negocio (simulacros) • Stock de repuestos sensibles para la operación. • Capacidad de mantenimiento oportuno. • Implementación interna de circuitos cerrados de televisión. • Monitoreo de conductas sospechosas. • Desconcentración de poder en la operación de equipos. • Cero tolerancia con la comisión de la conducta (denuncia) 	

Trata de personas	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 215
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Explotación sexual • Explotación laboral • Mendicidad ajena • Matrimonio servil 	
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas claras con los empleados. • Entrenamiento sensibilización de la modalidad delictiva y sus consecuencias penales, administrativas y traumatismo logístico a la operación. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. • Ejercer la actividad de su negocio en los parámetros legales éticos y de competencia leal. 	

Secuestro Extorsivo

Ley 599 del 2000 C.P y otras normas sancionatorias:

Art. 169 CP
Ley 733 de 2002

Tipología / modalidad delictiva:

- Arrebate, sustraiga, retenga u oculte a una persona con el propósito de exigir por su libertad un provecho o cualquier utilidad.
- Por grupo subversivo.
- Por delincuencia común.
- Autosequestro.

Procesos más vulnerables:

- Directivos
- Administrativos
- Operativos

Medidas de mitigación y continuidad de negocio:

- Diagnóstico y tratamiento de riesgo personal a los funcionarios que por su posición económica, de representatividad, exposición en zonas críticas y vulnerabilidad estén expuestas a posibles retaliaciones de grupos ilegales.
- Estudios de seguridad al personal en preempleo, rutina y específicos.
- Diagnóstico y tratamiento de riesgo personal a los funcionarios que por su posición económica, de representatividad, exposición en zonas críticas y vulnerabilidad estén expuestas a extorsión.
- Políticas de autocuidado y autoprotección.
- Control de manejo de redes sociales.
- Comunicaciones efectivas con las autoridades en especial DIASE.
- Política "Yo no pago, yo denuncio".
- Entrenamiento prevención delitos informáticos y seguridad de la información.
- Designación de responsable y campañas en protección de datos.
- Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales.
- Evite excesos de confianza, rutinas, transportar cuantiosas cifras de dinero, actitudes suntuosas, exposición de información privada.
- Evite zonas de riesgo.
- Dispositivos y medidas de seguridad que obedezcan a estudio de seguridad personal.
- No cargar información sensible o confidencial en dispositivos móviles o portátiles, tenga siempre presente lo que podría pasar si se le perdiera o fuese revisado de manera no consentida
- Tenga instalado la aplicación POLIS (sincronizar su celular con el celular del cuadrante correspondiente a su ubicación).
- Suministre la información estrictamente básica en su tarjeta de presentación personal.
- Asegúrese que siempre alguien de confianza conozca su ubicación y agenda que realiza.
- Dé instrucción a su familia y personal de servicio para que no suministren información personal que se considere sensible.
- Si considera que tiene nivel de riesgo considerable, debe generar un plan de retroalimentación periódica que incluya su entorno familiar y laboral más cercano.
- Si cuenta con personal de conductores o escoltas, valide su acreditación y competencia en manejo de armas, conducción reactiva y preventiva.

Soborno transnacional	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 433
Tipología / modalidad delictiva:	
Nacional o residente habitual en el país y con empresas domiciliadas en el mismo, ofrezca a un servidor público de otro Estado, directa o indirectamente, cualquier dinero, objeto de valor pecuniario u otra utilidad a cambio de que este realice u omita cualquier acto en el ejercicio de sus funciones, relacionado con una transacción económica o comercial.	
Procesos más vulnerables:	Directivo Administrativo
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Política de transparencia y cero tolerancia con la delincuencia. • Entrenamiento y sensibilización a empleados, consecuencias jurídicas. • No hacer mal uso de la posición dominante sobre el empleado. • La posición de Reverencia y subordinación del empleado hacia el empleador no le exime de responsabilidad penal. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Suplantación de sitios web para capturar datos personales	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 269 G
Tipología / modalidad delictiva:	
• Phishing (suplantación de sitios Web para capturar datos personales de la víctima)	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas de seguridad en la información (manejo de contraseñas, asignación de dominios individuales, actas de confidencialidad, apagado de equipo, clasificación de información, informe oportuno de novedades, guardado bajo llave de documentos impresos, escritorios y pantallas limpias, uso exclusivo de equipos de la empresa, controles de seguridad de instalaciones, no prestar usuarios, etc.). • Entrenamiento prevención de delitos informáticos y seguridad de la información. • Designación de responsable y campañas en protección de datos. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Actualización antivirus y FireWire. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Testaferrato**Ley 599 del 2000 C.P y otras normas sancionatorias:**

Art. 326

Tipología / modalidad delictiva:

- Quien preste su nombre para adquirir bienes con dineros provenientes del delito de narcotráfico y conexos.
- Cuentas bancarias
- Adquisición bienes inmuebles
- Constitución de empresas
- Adquisición de acciones
- Operaciones mercantiles
- Operaciones off shore

Procesos más vulnerables:

Directivo
Administrativo

Medidas de mitigación y continuidad de negocio:

- Estudios de seguridad a asociados de negocio.
- El tamaño de la empresa no determina el grado de vulnerabilidad, todas están expuestas.
- Manejo de la guía de control de riesgos financieros (ONU NRS).
- Adopción política conozca su cliente.
- Implementación de modelos de mitigación de riesgos LA/FT. (OEA, SIPLAF, BASC, etc.).
- Designación de Oficial de Cumplimiento.
- Control en la delegación de funciones (evitar concentración de poder y excesos de confianza en los empleados)
- Estudio y monitoreo de estados financieros.
- Acuerdos mutuos de seguridad.
- Capacitación y sensibilización de las consecuencias penales administrativas y reputacionales dirigido especialmente a los cargos de manejo y confianza.
- Política de legalidad y cero tolerancia con la delincuencia liderada por socios y nivel directivo.
- Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN.
- Protocolos de seguridad para admisión y monitoreo de accionistas.
- Implementación de estándares internacionales financieros.
- Gestión comercial directa (evitar intermediación informal o dudosa)
- Sinceridad tributaria ante la DIAN.

Tráfico de sustancias para procesamiento de narcóticos

Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 382 CP Ley 30 de 1986 Decreto Ley 19 de 2012 Resolución 0009 de 1987 Decreto 2272 de 1991
Tipología / modalidad delictiva:	
Mediante desvío, tráfico y uso ilícito de sustancias destinadas a la industria química. Mercado negro de sustancias químicas y precursores.	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Estudios de seguridad a asociados de negocio. • El tamaño de la empresa no determina el grado de vulnerabilidad, todas están expuestas. • Manejo de trazabilidad • Adopción políticas, conozca su cliente. • Implementación de modelos de mitigación de riesgos (OEA, BASC, ISO 28000, etc.). • Designación de responsable control • Control en la delegación de funciones (evitar concentración de poder y excesos de confianza en los empleados) • Estudio y monitoreo de vulnerabilidades. <ul style="list-style-type: none"> • Acuerdos mutuos de seguridad. • Capacitación y sensibilización de las consecuencias penales administrativas y reputacionales dirigido especialmente a los cargos sensibles. • Política de legalidad y cero tolerancia con la delincuencia liderada por socios y nivel directivo. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Usurpación de marcas y patentes

Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 306
Tipología / modalidad delictiva:	
Utilización fraudulenta de nombre comercial, enseña, marca, patente de invención, modelo de utilidad o diseño industrial protegido legalmente o similarmente confundible.	
Procesos más vulnerables:	Directivos Administrativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Adopción de negocios responsables éticos y legales. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. • Cero tolerancia con la comisión de la conducta (denuncia). • Control y monitoreo a cumplimientos legales y supervisión de entidades públicas. (Superintendencia de Industria y Comercio). • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Entrenamiento sensibilización de la modalidad delictiva y sus consecuencias penales, administrativas y traumatismo logístico a la operación. • Evitar vínculo de negocio que fomente esta actividad ilegal. 	

Tráfico, fabricación o porte de estupefacientes**Ley 599 del 2000 C.P y otras normas sancionatorias:**Art. 376 CP Ley 30 de 1986
Decreto 3788 de 1986
Decreto 2467 de 2015**Tipología / modalidad delictiva:**

- Tráfico clandestino vía aérea aerolíneas internacionales (aeropuertos clandestinos ilegales) marítima (lanchas rápidas, submarinos, Buques de carga internacional) y terrestre (empresas de transporte de pasajeros).
- Tráfico por contaminación de mercancías (camuflaje), maleta de doble fondo, cuadros, utensilios de aseo, adherido a las pachas partes mecánicas de tractocamiones, diluidas en sustancias, camuflada en contenedores, repatriación de cadáveres, entre otras.
- Correos humanos (mulas) adheridos, injeridos.

Procesos más vulnerables:Directivos
Administrativos
Operativos**Medidas de mitigación y continuidad de negocio:**

- Estudios de seguridad asociados de negocio.
- El tamaño de la empresa no determina el grado de vulnerabilidad, todas están expuestas.
- Manejo de trazabilidad
- Adopción de políticas, conozca su cliente.
- Implementación de modelos de mitigación de riesgos (OEA, BASC, ISO 28000, etc.).
- Designación de responsable control
- Control en la delegación de funciones (evitar concentración de poder y excesos de confianza en los empleados).
- Estudio y monitoreo de vulnerabilidades.
- Acuerdos mutuos de seguridad.
- Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN.

Violación de la libertad de trabajo**Ley 599 del 2000 C.P y otras normas sancionatorias:**

Art. 198

Tipología / modalidad delictiva:

- Con violencia o maniobra engañosa logre el retiro de operarios o trabajadores de los establecimientos donde laboran, o por los mismos medios perturbe o impida el libre ejercicio de la actividad de cualquier persona.

Procesos más vulnerables:Directivos
Administrativos**Medidas de mitigación y continuidad de negocio:**

- Dar garantías legales a los derechos de libertad al trabajo y no promover cultura de informalidad o arbitrariedad a sus empleados.

Transferencia no consentida de activos	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 269J CP Ley 1273 de 2009
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Phishing (suplantación de sitios Web para capturar datos personales de la víctima) • Skimming (Conducta que consiste en la clonación de tarjetas débito y crédito) • Ingeniería social (práctica social de obtener información a través del engaño) 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas de seguridad en la información (manejo de contraseñas, asignación de dominios individuales, actas de confidencialidad, apagado de equipo, clasificación de información, informe oportuno de novedades, guardado bajo llave de documentos impresos, escritorios y pantallas limpias, uso exclusivo de equipos de la empresa, controles de seguridad de instalaciones, no prestar usuarios, etc.). • Entrenamiento prevención de delitos informáticos y seguridad de la información. • Designación de responsable y campañas en protección de datos. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Actualización antivirus y FireWire. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Del tráfico de personas	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 188
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Violación de controles migratorios en frontera • Por intermedio de organizaciones criminales transnacionales (coyotes) • Por transporte marítimo clandestino • En buques de carga internacional (polisones) • Mediante suplantación de identidad (falsedad de documentos) 	
Procesos más vulnerables:	Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas claras con los empleados. • Entrenamiento sensibilización de la modalidad delictiva y sus consecuencias penales, administrativas y traumatismo logístico a la operación. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Uso de documento falso	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 291
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Acreditando calidad o título supuesto. • Como parte del fraude para una estafa. 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Cultura de gestión y control interno. • Adopción de políticas de corresponsabilidad penal. • Adopción de negocios responsables éticos y legales. • Cero tolerancia con la comisión de la conducta ilegal • Cultura de transparencia en participación de licitaciones. • Especial cuidado y mantenimiento con sus documentos de identidad. • Garantizar la trazabilidad y manejo de documentos mediante el registro documentado. • La posición de Reverencia y subordinación del empleado hacia el empleador no le exime de responsabilidad penal. • Manejo de políticas de confidencialidad a la información del personal y clientes administrada en el ejercicio del negocio correspondiente. • No pagar comisiones a tramitadores e intermediarios. • Política de cero tolerancia corporativas con la delincuencia. 	

Uso de software malicioso	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 269E CP Ley 1273 de 2009
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Malware (Programa informático que ejecuta acciones ilegítimas y desautorizadas en un sistema informático) • APT (ataques persistentes avanzados a través de phishing o correos dirigidos para obligar a un usuario para que ingrese a enlaces o archivos fraudulentos). • Spyware (Programa informático empleado para espiar sistemas electrónicos). • Ransomware (Programa informático empleado por los delincuentes para cifrar la información contenida en un computador y luego pedir recompensa). 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Políticas de seguridad en la información (manejo de contraseñas, asignación de dominios individuales, actas de confidencialidad, apagado de equipo, clasificación de información, informe oportuno de novedades, guardado bajo llave de documentos impresos, escritorios y pantallas limpias, uso exclusivo de equipos de la empresa, controles de seguridad de instalaciones, no prestar usuarios, etc.). • Entrenamiento para la prevención delitos informáticos y seguridad de la información. • Designación de responsable y campañas en protección de datos. • Política de control de respuestas a destinatarios desconocidos y solicitudes inusuales. • Actualización antivirus y FireWire. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Uso ilegítimo de patentes	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 307
Tipología / modalidad delictiva:	
Fabricar producto sin autorización de quien tiene el derecho protegido legalmente.	
Procesos más vulnerables:	Directivos Administrativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Adopción de negocios responsables éticos y legales. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. • Cero tolerancia con la comisión de la conducta (denuncia) • Control y monitoreo a cumplimientos legales y supervisión de entidades públicas. (Superintendencia de Industria y Comercio) • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Entrenamiento en sensibilización de la modalidad delictiva y sus consecuencias penales, administrativas y traumatismo logístico a la operación. • Evitar el vínculo de negocio que fomenta esta actividad ilegal. 	

Utilización indebida de fondos captados del público	
Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 314
Tipología / modalidad delictiva:	
Adquisición de acciones de entidades vigiladas y no vigiladas. Prohibición a los establecimientos bancarios de financiar a un tercero con dinero captado del público para adquirir el control de una entidad perteneciente o no al mismo sector.	
Procesos más vulnerables:	Directivos Administrativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Cero tolerancia con la comisión de la conducta (denuncia) • Control y monitoreo a cumplimientos legales y supervisión de entidades públicas. (Superintendencia de Industria y Comercio) • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Adopción de negocios responsables éticos y legales. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. 	

Utilización indebida de información privilegiada

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 258
Tipología / modalidad delictiva:		
Hacer uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público, por parte de empleado o directivos o miembros de una junta u órgano de administración de cualquier entidad privada, con el fin de obtener provecho para sí o para un tercero.		
Procesos más vulnerables:		Administrativos Operativos
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Entrenamiento en prevención de delitos informáticos y seguridad de la información. • Estudios de seguridad para seguimiento a personal interno que ostente cargo sensible (acceso a información y activos). • Manejo políticas de confidencialidad a la información del personal y clientes administrada en el ejercicio del negocio correspondiente. • Políticas de seguridad en la información (manejo de contraseñas, asignación de dominios individuales, actas de confidencialidad, apagado de equipo, clasificación de información, informe oportuno de novedades, guardado bajo llave de documentos impresos, escritorios y pantallas limpias, uso exclusivo de equipos de la empresa, controles de seguridad de instalaciones, no prestar usuarios, etc.). 		

Violación a los derechos morales de autor

Ley 599 del 2000 C.P y otras normas sancionatorias:		Art. 270
Tipología / modalidad delictiva:		
<ul style="list-style-type: none"> • Publicar, total o parcialmente, sin autorización previa y expresa del titular del derecho. • Inscribir en el registro de autor con nombre de persona distinta del autor verdadero. • Compendie, mutile o transforme, sin autorización previa o expresa de su titular. <p>Una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho.</p>		
Procesos más vulnerables:		Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:		
<ul style="list-style-type: none"> • Adopción de negocios responsables éticos y legales. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. • Cero tolerancia con la comisión de la conducta (denuncia) • Control y monitoreo a cumplimientos legales y supervisión de entidades públicas y privadas. (Superintendencia de Industria y Comercio, Dirección Nacional de Derechos de Autor, Cámara Colombiana del Libro). • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Entrenamiento sensibilización de la modalidad delictiva y sus consecuencias penales, administrativas y traumatismo logístico a la operación. • Evitar vínculo de negocio que fomente esta actividad ilegal. 		

Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones

Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 272
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Superar o eludir las medidas tecnológicas adoptadas para restringir los usos no autorizados. • Suprimir o alterar la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada. • Fabricar, importar, vender, arrendar o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal, o de cualquier forma de eludir, evadir, inutilizar o suprimir un dispositivo o sistema que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de estos. • Presentar declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación, liquidación o distribución de derechos económicos de autor o derechos conexos, alterando o falseando, por cualquier medio o procedimiento, los datos necesarios para estos efectos. 	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Adopción de negocios responsables éticos y legales. • Activa participación en las actividades organizadas por el Frente de Seguridad Empresarial DIJIN. • Cero tolerancia con la comisión de la conducta (denuncia). • Control y monitoreo a cumplimientos legales y supervisión de entidades públicas y privadas. (Superintendencia de Industria y Comercio, Dirección Nacional de Derechos de Autor, Cámara Colombiana del Libro). • Denunciar a las autoridades si se tiene conocimiento de la práctica comercial ilegal. • Entrenamiento en sensibilización de la modalidad delictiva y sus consecuencias penales, administrativas y traumatismo logístico a la operación. • Evitar vínculo de negocio que fomente esta actividad ilegal. 	

Violación de datos personales

Ley 599 del 2000 C.P y otras normas sancionatorias:	Art. 269F CP Ley 1273 del 2009 Ley 1581 del 2012
Tipología / modalidad delictiva:	
<ul style="list-style-type: none"> • Obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes. <p>Sin estar facultado para ello, con provecho propio o de un tercero.</p>	
Procesos más vulnerables:	Directivos Administrativos Operativos
Medidas de mitigación y continuidad de negocio:	
<ul style="list-style-type: none"> • Implementar y respetar la Ley 1581 del 2012 Habeas Data. • Manejo de políticas de confidencialidad a la información del personal y clientes administrada en el ejercicio del negocio correspondiente. 	

Violación de los derechos de reunión y asociación**Ley 599 del 2000 C.P y otras normas sancionatorias:** Art. 200**Tipología / modalidad delictiva:**

Impedir o perturbar una reunión lícita o el ejercicio de los derechos que conceden las leyes laborales o tome represalias con motivo de huelga, reunión o asociación legítimas.

Procesos más vulnerables:

Directivos
Administrativos

Medidas de mitigación y continuidad de negocio:

Fomentar las buenas relaciones laborales y contribuir a la solución de los conflictos colectivos de trabajo, respetando el derecho de expresión colectiva de los empleados.

Violación de medidas sanitarias**Ley 599 del 2000 C.P y otras normas sancionatorias:** Art. 368**Tipología / modalidad delictiva:**

Violar medida sanitaria adoptada por la autoridad competente para impedir la introducción o propagación de una epidemia

Procesos más vulnerables:

Directivos
Administrativos
Operativos

Medidas de mitigación y continuidad de negocio:

- Control y monitoreo a cumplimiento de legales y supervisión de entidades públicas y privadas. (INVIMA, Secretaría de Salud, Ministerios etc.).

Violación de reserva industrial o comercial**Ley 599 del 2000 C.P y otras normas sancionatorias:** Art. 308**Tipología / modalidad delictiva:**

Emplear, revelar o divulgar descubrimiento, invención científica, proceso o aplicación industrial o comercial, llegados a su conocimiento por razón de su cargo, oficio o profesión y que deban permanecer en reserva.

Procesos más vulnerables:

Administrativos
Operativos

Medidas de mitigación y continuidad de negocio:

- Entrenamiento en prevención de delitos informáticos y seguridad de la información.
- Estudios de seguridad para seguimiento a personal interno que ostente cargo sensible (acceso a información y activos).
- Manejo de políticas de confidencialidad a la información del personal y clientes administrada en el ejercicio del negocio correspondiente.

1.4 Entorno de la seguridad, riesgo actual y su impacto en la cadena de suministro



“Las empresas de la nueva era deben asegurar la integridad de sus prácticas de seguridad”.



Los desafíos de la seguridad y la gestión del riesgo varían en cada región y de una empresa a la otra; igualmente, cambia en cada equipo que trabaja por minimizar la ocurrencia de una pérdida y se manifiesta de diferentes formas, depende de las condiciones, metas y necesidades de cada negocio; no se puede hablar de estándar de seguridad para toda Latinoamérica sin antes evaluar cada país, pero sí se puede trazar una línea de analogía entre los hechos que están ocurriendo, las falencias del sector, los casos negativos y los métodos que de manera positiva ayudan a salir adelante contra el crimen en la actividad económica que desarrollamos.

El riesgo es inherente a toda tarea realizada por los seres humanos y de él no se escapa ninguna actividad empresarial; partiendo de la premisa que es mejor estar preparado para algo que quizás no suceda a que suceda algo y nos coja por sorpresa por no haber estado preparados; es necesario prever con la suficiente anticipación la probabilidad de ocurrencia de riesgos, que de llegar a presentarse, pueden afectar los intereses empresariales e incluso amenazar la continuidad del negocio, anticiparnos a los acontecimientos y estar preparados con planes de contingencia para afrontar los eventos no deseados (y que pueden tener), con el potencial de interrumpir las operaciones y hasta impedir el desarrollo futuro del objeto social de la compañía.

La diversidad de riesgos que a menudo vienen afrontando las empresas involucradas en la cadena de suministro es cada vez mayor y se suman a los eventos naturales y a los riesgos que tienen origen en actividades criminales que son los de mayor ocurrencia, aquellos eventos originados en inconformidades sociales que pueden llegar a paralizar actividades de producción y transporte por prolongados espacios de tiempo, ocasionando severos daños económicos y, también, pérdida de la confianza con clientes y proveedores por incumplimiento en plazos de entrega.

Los riesgos reputacionales también se hacen presente sobre todo en zonas donde la conflictividad conlleva amenazas de diferentes grupos delictivos que además atacan instalaciones, personas y vehículos para presionar el pago de sumas extorsivas que, si

logran su objetivo y obtienen el pago, en ocasiones exponen a las empresas ante las autoridades y la opinión pública como promotores de la violación de los derechos humanos o de ser financiadores de la delincuencia y el terrorismo. Los grandes capitales que mueven las actividades del narcotráfico, también, a veces permean a las personas involucradas en algún eslabón de la cadena de suministro, y si los controles no son eficaces, no sólo se presenta el riesgo reputacional sino también el de ser tildados como responsables de lavado de activos, con todas las consecuencias negativas que esto conlleva y que pueden, incluso, sacar del mercado a una empresa.

No basta con mantener unos excelentes estándares y contemplar el paso a paso de la gestión del riesgo, porque a pesar de contar con todos los controles necesarios para gestionarlos, en este mundo cambiante y cada vez más globalizado, surgen nuevas modalidades delictivas, nuevos riesgos; como por ejemplo, aquellos que pueden penetrar los sistemas informáticos de las compañías y que cada año vienen en aumento con el uso de internet y las transacciones a través de la red.

Además, se hace imperativo establecer un sistema que permita cerrar los ciclos, documentando e investigando los incidentes que hayan ocasionado efectos negativos, compartiendo y estudiando la casuística para conocer tendencias, nuevas modalidades y, lo más importante, divulgar las lecciones aprendidas para poder establecer mecanismos de anticipación y poder contar con alternativas para mitigar los efectos perjudiciales y con unos

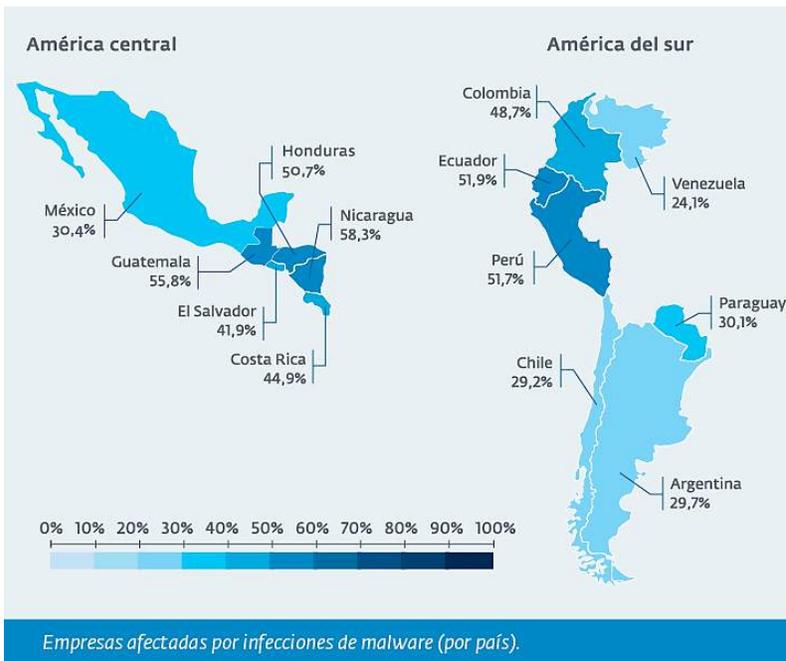
planes efectivos para reponerse a los eventos que llegaren a presentarse.

Acá es donde toma relevancia el concepto de “empresas resilientes”, que se refiere a la capacidad para recuperarse de una situación traumática, como por ejemplo, una crisis generada por la materialización del riesgo; si estamos preparados para dar una efectiva respuesta a una crisis o contingencia, el tiempo de recuperación será más corto y por ende menores las pérdidas, pero si como en algunos casos pensamos “esto no me pasa a mí” o se cuenta con la “sensación de invulnerabilidad”, un evento negativo podría tomarnos por sorpresa, la capacidad de recuperación sería insuficiente, la reacción tardía y los tiempos de respuesta efectiva serían más prolongados.

Las empresas de la nueva era deben asegurar la integridad de sus prácticas de seguridad y comunicar sus lineamientos a sus socios comerciales dentro de la cadena de abastecimiento, tomar un papel activo en la guerra contra la delincuencia y el terrorismo y reconocer que se debe facilitar la circulación del comercio legítimo; el entorno actual es, entonces, muy evidente, más cantidad de información personal y empresarial disponible en internet, brechas de seguridad desconocidas por evolución y la implementación de nuevas tendencias, nuevos desafíos para proteger el negocio, donde no se debe dejar de lado la preparación continua de ninguno empleado, de ningún funcionario, a su vez, la combinación de la gestión con la educación y específicamente hacia las nuevas tecnologías, aquellas que

agobiaron de un momento a otro el manejo de la información y que vulneran la confidencialidad de la misma, al dejarla en manos de equipos inexpertos en su manejo o de los mal llamados “expertos desconocidos”.

Es evidente, también, que desde la inclusión en un registro de ingreso o salida, el movimiento de una carga, la trazabilidad de la misma, como también el arribo a los diferentes puntos de control, son actualmente monitoreados por equipos móviles y los engaños y trampas nacen a diario; actualmente, los incidentes de seguridad en este importante sector son proporcionalmente directos al crecimiento y la introducción de las nuevas tecnologías en cada país; por ejemplo, Colombia tiene 48,7% de empresas que han sido afectadas con infecciones malware y que, según cifras del Eset Security Report, 2016, frente a Chile con 29,2% y Perú con un 51,7%, determina que debemos orientar nuestros esfuerzos a la seguridad de las nuevas tendencias en las que se desarrollan los trabajos y tomar las acciones correctas para proteger la información, con ello se definen alertas, reportes y procesos para las acciones que ayuden a disminuir la cantidad de eventos y vulnerabilidades, pues ahora son más de un 87% de nuestras operaciones que están siendo manejadas por equipos informáticos.



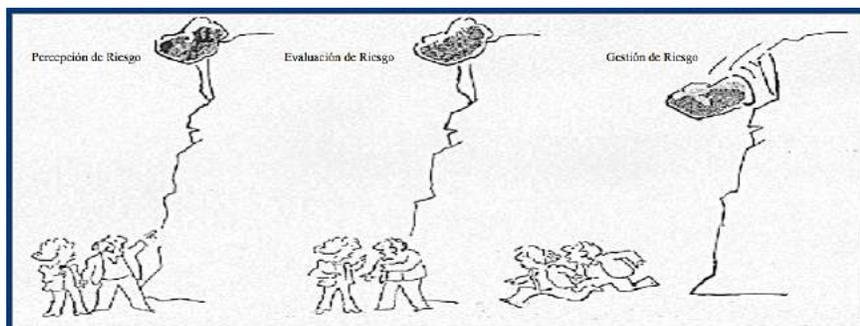
Fuente: ESET Security Report, 2016.

En la actualidad, las amenazas además de venir del exterior, nacen desde el interior de la organización; si mencionamos la introducción de las redes sociales a los equipos de las compañías, podemos observar que según un estudio de

Adalid Compañía, una consultora de seguridad informática en Colombia, “existe una tendencia que demuestra que el 80% de adultos que tienen redes sociales navegan torpemente en ellas” y es que la seguridad y privacidad en línea ya no son una problemática de pocos, se han convertido en parte integral de nuestras vidas y de nuestras empresas; el cibercrimen representa el 15% de los ilícitos cometidos a empresas en Colombia y genera pérdidas anuales cercanas a los 600 millones de dólares, debemos romper las fronteras del profesional de la seguridad y enfatizar en la prevención del crimen en nuestras compañías, incluyendo la evaluación y diseño de panoramas de riesgo con inclusión de este nuevo escenario por ciberdelincuencia, mantenernos en avance e investigación hacia la innovación de los diferentes panoramas que se producen, tanto en Colombia como en el ámbito internacional.

Esta es la primera tarea, llevar a cabo un análisis de riesgo de la cadena de suministro y el estado actual, ya que este es críticamente importante, permite a los socios verdaderamente conocer vulnerabilidades dentro de la cadena logística y determinar qué hacer con el fin de mitigar los riesgos identificados; uno de los modelos de gran auge ha sido el “Análisis de Riesgos en 5 Pasos”, herramienta publicada por el programa Customs – Trade Partnership Against Terrorism, C-TPAT, y que no exige una técnica específica para llevar a cabo el análisis de riesgo, pero lo ejemplariza de la siguiente manera, basado a la manera en la que opere su negocio:

1. Mapear el flujo del embarque e identificar los socios comerciales (contratados directamente o indirectamente).
2. Realizar un análisis de riesgo y amenazas: clasificar el riesgo - Alto, Medio, Bajo.
3. Realizar un análisis de vulnerabilidad y clasificar la vulnerabilidad - Alto, Medio, Bajo.
4. Elaborar un Plan de Acción y Seguimiento.
5. Documentar cómo se realizan los análisis de riesgo.



Fuente: *Análisis de riesgo de la cadena de suministro internacional C-TPAT International Branch, Washington, D.C. Homeland Security*

Aristides Contreras Fernández, Orlando Hernández Angarita

Directivos Comunidad latinoamericana de consultores y asesores en Gestión de riesgo y seguridad, COLADCA

1.5 Perspectivas de la Seguridad empresarial



1.5.1 Desde la opinión de diferentes actores de la cadena de suministro. (Aplicación de encuestas)



Encuesta No. 1. Victimización vs. Afectación de pólizas

Con la intención de conocer la realidad subjetiva de victimización y modalidades más recurrentes de la criminalidad que afectan las operaciones productivas en Colombia, el Frente de Seguridad Empresarial de la DIJIN lidera un escenario denominado Mesa técnica por sectores. Dentro de la agenda y plan de actividades se realiza una trimestral de acuerdo con el frente de cobertura más interesado. En este orden, las mesas técnicas con enfoque al sector transporte, tradicionalmente convocan la mayor cantidad de empresas de este sector, pero también una muestra representativa de los demás actores de la cadena de suministro que interactúan con este, lo que da más peso a la evolución que han tenido las cadenas de valor frente a la necesidad de generar un idioma de entendimiento trazable, basado en la efectividad de sus controles.

Así las cosas, el pasado 30 de junio se realizó la segunda mesa técnica del año orientada a los actores de la cadena de suministro, con el fin de aplicar un instrumento tipo encuesta de percepción, que permitiera generar una mayor rigurosidad tipo estudio, como insumo para la Guía. Sus resultados fueron tabulados y puestos a consideración en esta publicación, como un insumo de apreciación integral de los fenómenos delictivos recurrentes, así como del aseguramiento del riesgo de seguridad materializado y la gestión frente a las aseguradoras para mitigar el impacto del mismo. Estos fueron los resultados:



FICHA TÉCNICA



Aplicada el 30 de junio de 2016 en el marco de la reunión de la Mesa transportadores realizada en Bogotá.



Universo, **77** empresas de transporte que hacen parte de FESEM.

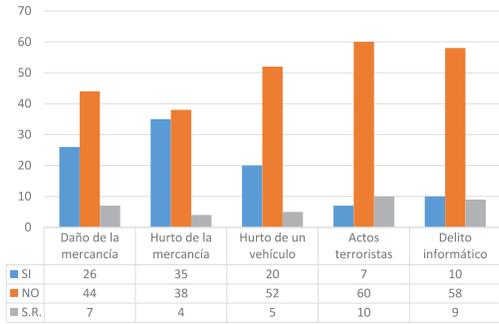


Metodología, encuesta directa a empresas de transporte con respuesta única y múltiple.

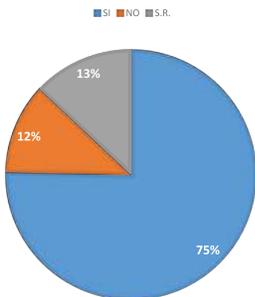


Evaluación de seguridad para las empresas transportadoras.

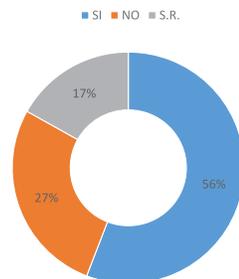
1. En sus operaciones de los últimos dos años, su compañía presentó algunos de los siguientes eventos y/o siniestros:

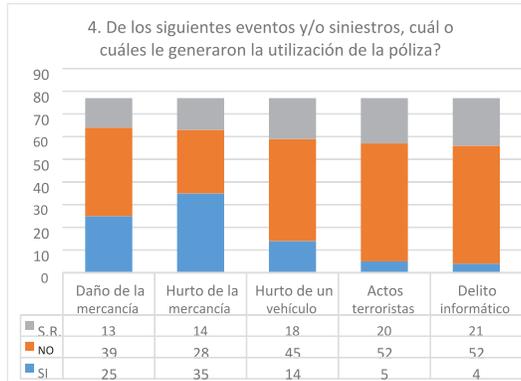


2. Durante los eventos y/o siniestros que tuvo, La empresa contaba con una póliza de seguro?



3. De los eventos o siniestros que tuvo en los dos años, estando asegurado, ¿la empresa realizó el reclamo a la aseguradora?





Conclusiones de la encuesta



- En los dos últimos años, las operaciones de las empresas encuestadas fueron en su orden de mayor a menor, frecuentemente afectadas por hurto de mercancías, con 36 casos, seguido del daño de mercancías con 24 eventos y los delitos por medios informáticos con 10 reportes.
- La mayoría de las empresas consultadas, es decir, el 75% de las empresas reportaron tener asegurado el riesgo mediante amparo con firma aseguradora, lo que permite evidenciar el conocimiento del riesgo y la importancia que dedican contemplándolo como críticos para solicitar el pago de la póliza.
- El 56% afectó la póliza por causa del impacto de los riesgos y un 27% asumió los impactos económicos correspondientes.
- En la misma línea de análisis, las empresas consultadas reportaron haber utilizado la póliza con mayor frecuencia por haber sido víctima de hurto de mercancías; este delito se registra como el evento que motivó el mayor número de victimizaciones y en la misma forma la afectación de pólizas, seguido por el daño de mercancías, con 25 eventos reportados en la encuesta aplicada.





Encuesta No. 2. Medición de percepción de seguridad empresarial

Con el fin de tener acceso a otros elementos de información y la opinión de los empresarios en Colombia, potenciales y en algunos casos víctimas de la criminalidad con afectación empresarial, apoyados con las herramientas tecnológicas disponibles y prácticas, se aplicó una segunda encuesta en forma virtual, dirigida a una muestra representativa de empresas vinculadas al Frente; con el objetivo de conocer el nivel de victimización, el impacto del riesgo materializado, la identificación previa del mismo, el nivel de denuncia, la adopción y efectividad de planes de continuidad, como una forma de identificar el grado de interés sobre la prevención criminal, el conocimiento del proceso más vulnerable y el tipo de delito que más les preocupa como amenazas desde la perspectiva actual del contexto criminal vigente y de la identificación eficiente del riesgo y la conciencia de tener una gestión adecuada frente al potencial riesgo de ser víctima.

FICHA TÉCNICA



Aplicada el 26 de julio del 2016.



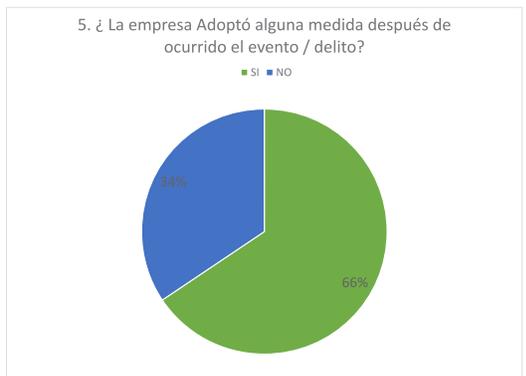
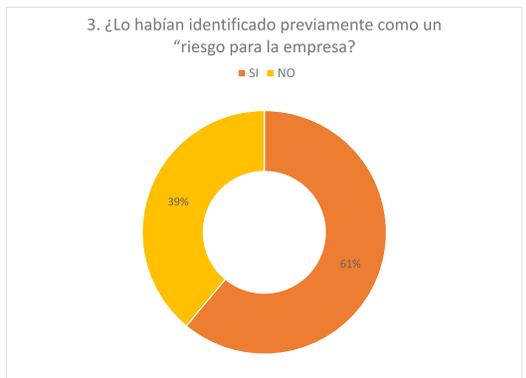
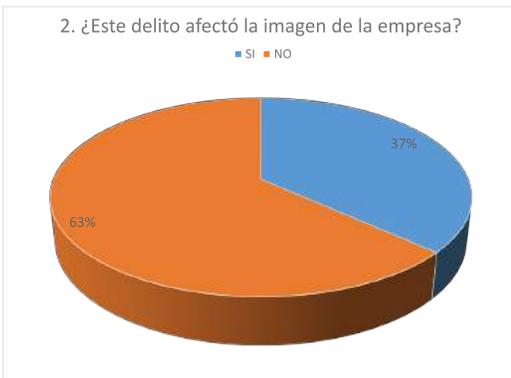
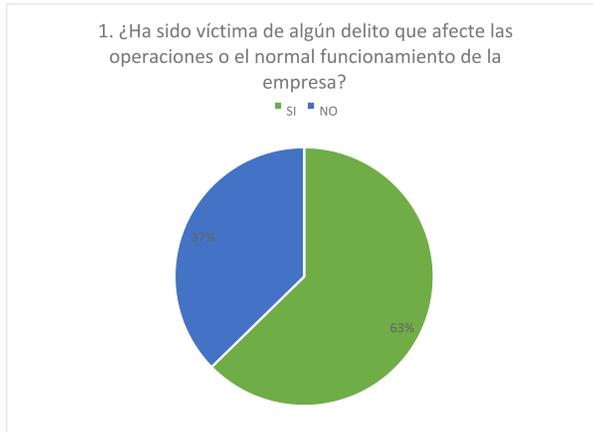
Universo, 308 empresas que hacen parte de FESEM.

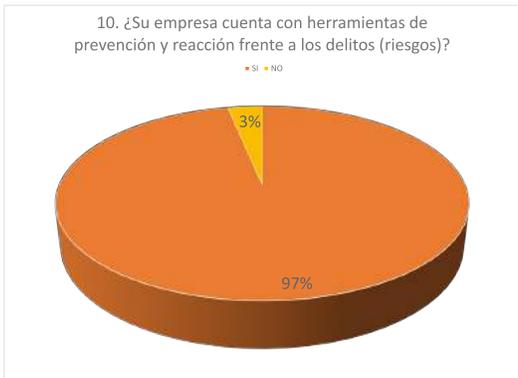
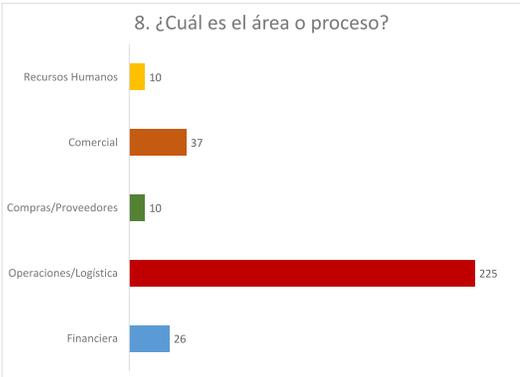
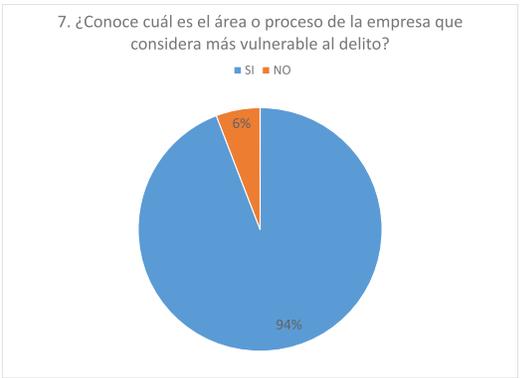
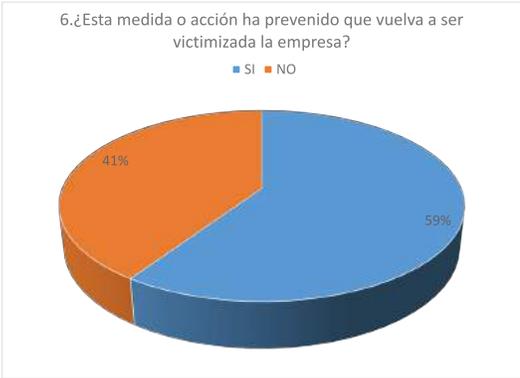


Metodología, encuesta virtual con respuesta única y múltiple. Aplicación Google Docs.



Percepción de seguridad.





Conclusiones de la encuesta

- Con el objetivo de conocer el impacto del riesgo materializado, la identificación previa del mismo, el nivel de denuncia, la adopción y efectividad de planes de continuidad, como una forma de identificar el grado de interés sobre la prevención criminal, el conocimiento del proceso más vulnerable y el tipo de delito que más les preocupa como amenazas desde la perspectiva actual del contexto criminal vigente y de la identificación eficiente del riesgo y la conciencia de tener una gestión adecuada frente al potencial riesgo de ser víctima.
- Con un 63% de participación, la mayoría de la población de empresas encuestadas registra que el proceso de operaciones ha sido el más afectado por eventos de criminalidad, sin embargo, este porcentaje de eventos registrados no afectan la imagen de una compañía, gestionando en forma eficiente el riesgo reputacional, dado que previamente se identificó la criticidad y posteriormente se tomaron medidas o planes de continuidad.
- El 69% había identificado previamente el riesgo materializado, desde otra perspectiva, se infiere que se requiere mayor efectividad en las medidas de mitigación y prevención.
- Tan solo el 56% de las empresas, posterior a la materialización del riesgo, se cumplió con el deber legal de instaurar denuncia penal, lo cual es un porcentaje muy bajo, debido a que la política de las empresas en Colombia debería ser cero tolerancia a la delincuencia y el cumplimiento al 100% del deber de denunciar.
- El 66% de las empresas adoptó medidas, con posterioridad al evento, generando preocupación que el 34% restante no asumió un plan correctivo para tratar y mitigar las causas generadoras de riesgo, y aquellas que lo trataron manifestaron haber obtenido resultado preventivo en un 59% de efectividad.
- El 94% de las empresas consultadas manifiestan conocer sus procesos más vulnerables; siendo el proceso de operaciones/logística, la frecuentemente registrada con 225 reportes.
- Con 210 registros se destaca el hurto como el delito que más preocupa a los empresarios consultados, seguido por los delitos informáticos con 26 reportes.
- El 97% de la población consultada manifiesta tener implementadas herramientas de prevención y reacción frente a los delitos, lo cual es positivo, ya que evidencia conciencia frente a la importancia y necesidad de realizar una eficiente gestión del riesgo.

1.5.2 Análisis criminológico del Observatorio del Delito de la Policía Nacional

Con el fin de dar a conocer la criminalidad registrada, el Observatorio del Delito de la DIJIN presenta un análisis descriptivo de las cifras registradas en el aplicativo Sistema de Información estadístico, delincuencia, contravencional y operativo SIEDCO y Sistema de información de denuncias y contravenciones SIDENCO durante las dos últimas vigencias, de acuerdo con las denuncias efectuadas por los ciudadanos en Colombia y a la cobertura del servicio de policía, permitiendo conocer el contexto y comportamiento de los delitos frecuentemente dados a conocer a las autoridades con la expectativa de justicia u otras pretensiones.

En el siguiente análisis se describen las características comparativas de los delitos que afectan la seguridad pública y seguridad ciudadana a nivel país, periodo comparativo del 1° de enero al 31 de diciembre de los años 2014 y 2015.

Hurto a personas

Gráfico 1. Comparativo de hurto a personas, años 2014-2015.



Fuente: SIEDCO

El 60% de las víctimas son hombres (60.832 casos).

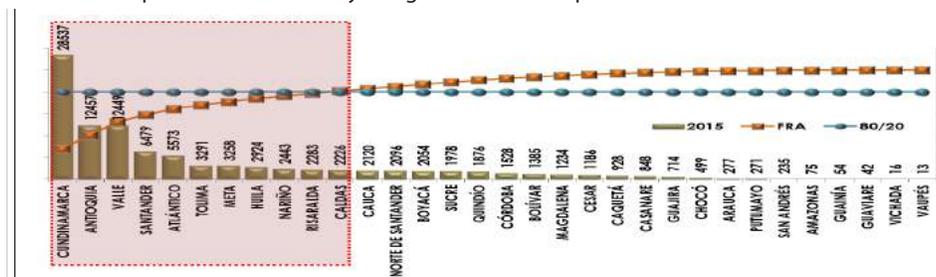
El arma de fuego se empleó en el 20% de los casos (19.838), seguido del arma corto-punzante con el 19% (19.245), es de anotar que en el 46% (46.801 hechos) no se emplearon armas.

El atraco con un 43% (43.201 casos) es la modalidad de mayor registro, seguido del raponazo con un 10% (10.247); siendo el factor de oportunidad el que más aporta con el 33% (33.517 hechos).

El día viernes es el de mayor participación con el 16% (15.731 casos).

El 35% de los hurtos a personas (35.490 casos), ocurren en el intervalo de hora comprendido de 12:00 a 17:59.

Gráfico 2. Departamentos con mayor registro de hurto a personas en el año 2015.

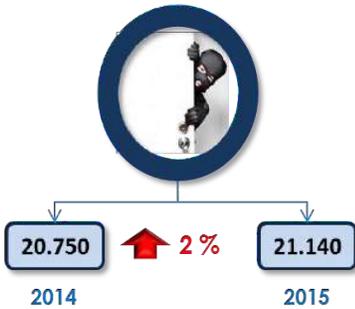


Fuente: SIEDCO

11 Departamentos concentran el 81% de los hurtos a personas, razón por la cual es importante el esfuerzo conjunto en estas zonas.

Hurto a residencias

Gráfico 3. Comparativo de hurto a residencias, años 2014-2015.



Fuente: SIEDCO

Los electrodomésticos con el 56% son los elementos más hurtados, seguidos de las joyas con el 20% y el dinero con el 18%.

Los días domingos y jueves son los de mayor participación con el 15% (3.183 y 3.135 casos cada uno).

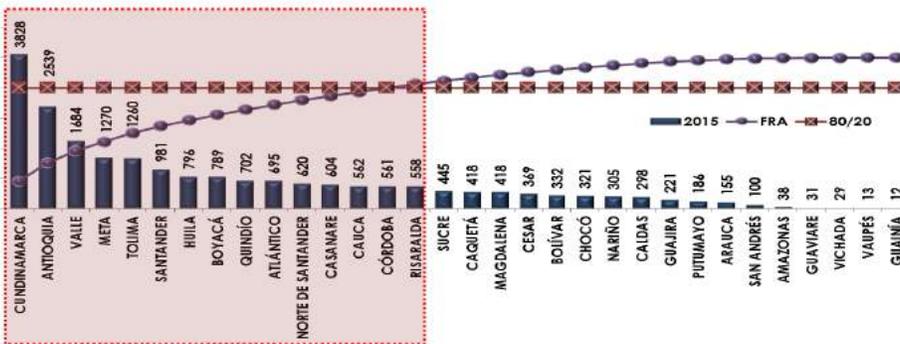
El mes de enero con un 10% (2.101 casos) es el de mayor registro.

Las armas contundentes se emplearon en el 41% de los casos (8.758), seguido del arma de fuego con el 8% (1.747), en el 45% (9.517 hechos) no se emplearon armas.

La violación de cerraduras con un 26% (5.422 casos) es la modalidad de mayor registro, seguido de la ventosa con un 18% (3.731), el factor de oportunidad aporta el 31% (6.487 hechos) de la totalidad de casos registrados.

El 29% de los hurtos a residencias (6.086 casos), ocurren en el intervalo de hora comprendido de 12:00 a 17:59.

Gráfico 4. Departamentos con mayor registro de hurto a residencias en el año 2015.



Fuente: SIEDCO

15 Departamentos concentran el 83% de los hurtos a residencias, lo que amerita fortalecer el trabajo conjunto de los cuadrantes con la vigilancia y seguridad privada que prestan sus servicios en estas jurisdicciones.

Hurto a comercio

Gráfico 5. Comparativo de hurto a comercio, años 2014-2015.



Fuente: SIEDCO

Los almacenes con el 28% (6.303 casos) son los más afectados por este delito, seguido de los locales comerciales con el 14% (3.041).

Los días lunes y viernes son los de mayor participación con el 15% (3.368 y 3.337 casos cada uno).

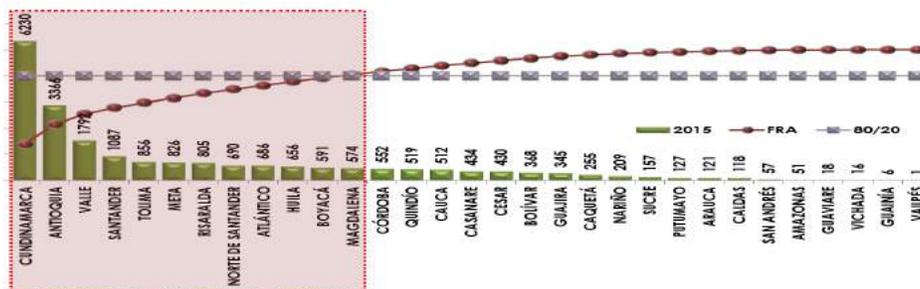
Los meses de abril y enero con un 9% (2.050 y 2.045 casos respectivamente) son los de mayor registro.

Las armas contundentes se emplearon en el 20% de los casos (4.571), seguido del arma de fuego con el 14% (3.045), en el 61% (13.608 hechos) de los casos registrados no se emplearon armas.

El mechero con el 21% (4.686 casos) es la modalidad de mayor registro, seguido del atraco con un 16% (3.674), es de anotar que el factor de oportunidad aporta el 39% (8.775 hechos).

El 33% de los hurtos a residencias (7.481 casos), ocurren en el intervalo de hora comprendido de 12:00 a 17:59.

Gráfico 6. Departamentos con mayor registro de hurto a comercio en el año 2015.

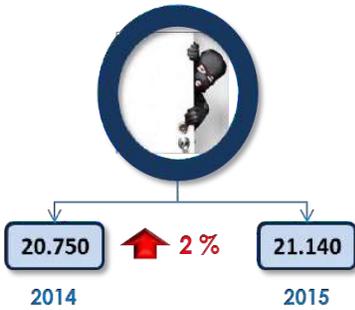


Fuente: SIEDCO

12 Departamentos concentran el 81% de los hurtos a comercio, de ahí que el intercambio de información con la Policía Nacional debe fortalecerse.

Hurto de automotores

Gráfico 7. Comparativo de hurto de automotores, años 2014-2015.



Fuente: SIEDCO

La marca más hurtada es la Chevrolet con el 32% (2.443 casos), seguida de la Mazda con el 15% (1.127) y la Hyundai con un 11% (815).

Los meses de agosto, febrero y noviembre con un 9% (693, 676 y 673

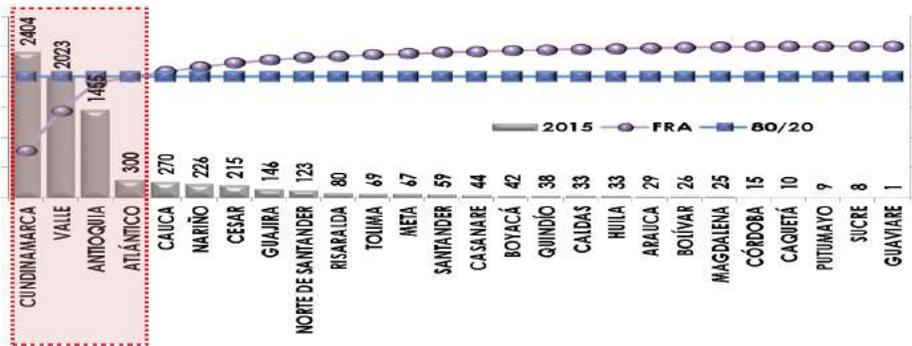
casos respectivamente) son los de mayor registro.

La llave maestra se empleó en el 66% de los casos (5.130), seguido del arma de fuego con el 26% (2.007) y las armas contundentes con el 4% (310 casos).

El halado con el 67% (5.212 casos) es la modalidad de mayor registro, seguido del atraco con un 27% (2.123) y el engaño con un 3% (228).

El 35% de los hurtos de automotores (2.688 casos), ocurren en el intervalo de hora comprendido de 18:00 a 23:59, seguido de las 12:00 a 17:59 y de 06.00 a 11:59 con un 26% (2.026 y 1.977 hechos respectivamente).

Gráfico 8. Departamentos con mayor registro de hurto de automotores año 2015.

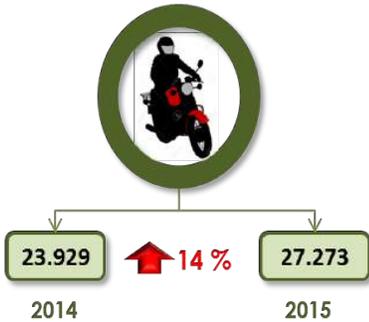


Fuente: SIEDCO

4 Departamentos concentran el 80% de los hurtos de automotores, factor de atención para la industria automotriz.

Hurto de motocicletas

Gráfico 9. Comparativo de hurto de motocicletas años 2014-2015.



Fuente: SIEDCO

La marca más hurtada es la Bajaj con el 29% (7.918 casos), seguido de la Yamaha con el 24% (6.554) y la Honda con un 13% (3.668).

Los meses de octubre y noviembre con un 9% (2.558 y 2.480 casos respectivamente) son los de mayor registro.

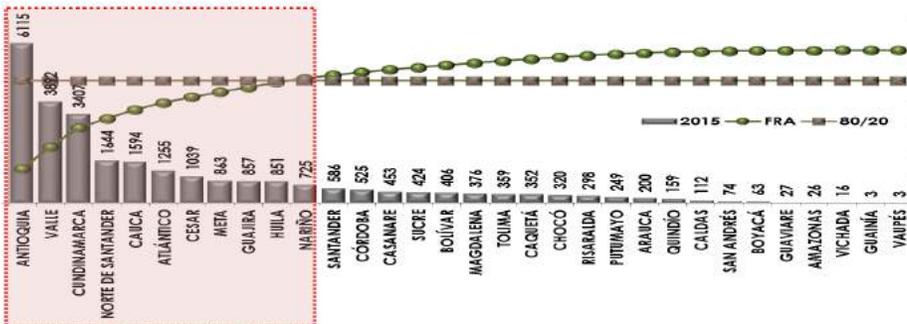
El 83% de las víctimas (22.541 casos) fueron hombres.

La llave maestra se empleó en el 47% de los casos (13.320), seguido del arma de fuego con el 33% (8.900) y las armas contundentes con el 5% (1.443 casos).

El halado con el 57% (15.436 casos) es la modalidad de mayor registro, seguido del atraco con un 38% (10.291), el factor de oportunidad descuido aporta el 4% (1.003 hechos) al consolidado nacional.

El 41% de los hurtos de automotores (11.100 casos), ocurren en el intervalo de hora comprendido de 18:00 a 23:59, seguido de las 12:00 a 17:59 con el 23% (6.393), de 06:00 a 11:59 con un 20% (5.439) y de 00:00 a 05:59 con el 16% (4.341).

Gráfico 10. Departamentos políticos con mayor registro de hurto de motocicletas año 2015.

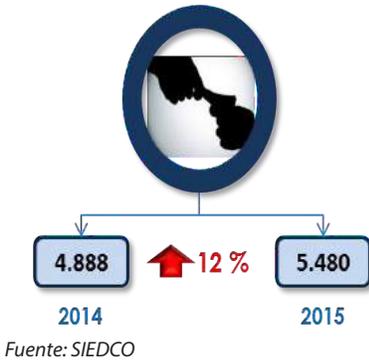


Fuente: SIEDCO

11 Departamentos concentran el 82% de los hurtos de motocicletas, análisis que tiene relación con el incremento de la comercialización de este tipo de transporte.

Extorsión

Gráfico 11. Comparativo de Extorsión, años 2014-2015.



El 64% de las víctimas (3.532 casos) fueron hombres.

Las armas contundentes se emplearon en el 61% de los casos (3.345), seguido de las armas blancas con el 10% (565), es de anotar que en el 25% (1.393 hechos) no se emplearon armas.

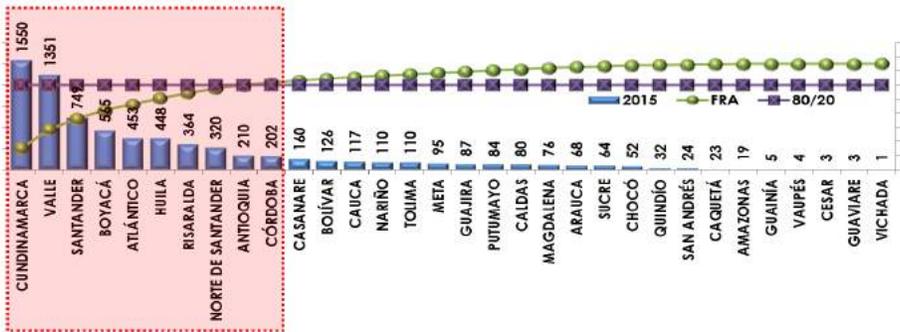
La llamada a celular con el 54 % (2.960 casos) fue la modalidad de mayor registro, seguido de la directa con el 20% (1.075) y la mixta con el 14% (771).

El 35% de las víctimas (1.899 hechos), son empleados particulares, seguido de los comerciantes con el 28% (1.530) y los agricultores con un 6% (530).

El 92% de las víctimas son los adultos con (5.041 hechos), seguido de los adolescentes con el 1% (57), cabe resaltar que en el 7% (363 casos) no se registra la edad de la víctima.

Los meses de enero y febrero con un 12% (652 y 650 casos respectivamente) son los de mayor registro.

Gráfico 12. Departamentos con mayor registro de extorsión año 2015.

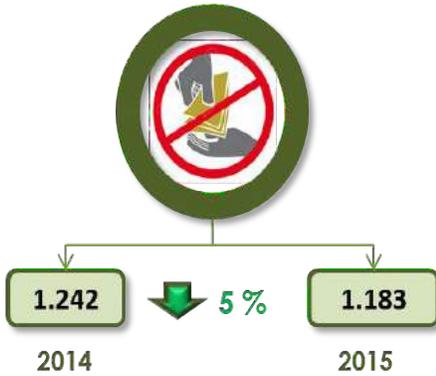


Fuente: SIEDCO

10 Departamentos concentran el 82% de hechos de estafa, análisis que debería tenerse en cuenta en los mapas de riesgos de las empresas.

Cohecho

Gráfico 17. Comparativo casos de cohecho, años 2014-2015.



Fuente: SIEDCO

El 13% de los implicados (151 casos) ostentaban el grado de patrullero, seguido de los subintendentes con el 2% (23) y los intendentes con el 1% (10), es de anotar que en el 84% (992 hechos) no se registra el grado del implicado.

El 97% (1.155 hechos) se presentaron bajo la modalidad de cohecho por dar u ofrecer,

seguido del cohecho propio con el 2% (20) y 8 hechos por cohecho impropio.

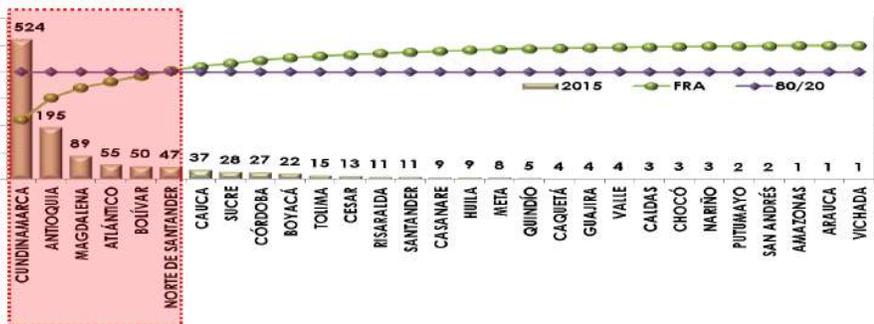
Los hombres con el 96% (1.133 casos) son los más implicados en este delito, mientras que en un 4% (50) fueron mujeres.

El 51% (602 casos) fueron registrados en la zona urbana, mientras que la rural se reportó el 49% (581).

El 49% (582 casos) fueron perpetrados en vías públicas, seguido de las carreteras con un 39% (458) y el 7% (81) en tramos viales.

El mes de mayo registra el mayor número de hechos con el 12% (137 hechos).

Gráfico 18. Departamentos con mayor registro de hechos de cohecho año 2015.

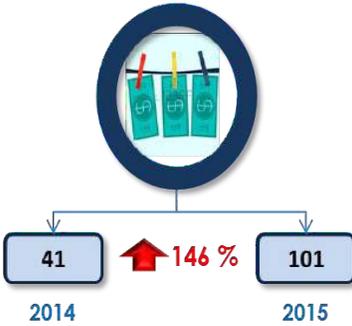


Fuente: SIEDCO

6 Departamentos concentran el 81% de casos de cohecho, lo que debe motivar la denuncia en estas jurisdicciones.

Lavado de activos

Gráfico 19. Comparativo de lavado de activos, años 2014-2015.



Fuente: SIEDCO

El 65% (66 casos) están relacionados con el narcotráfico, el 35% de los hechos restantes no están relacionados con un delito en específico.

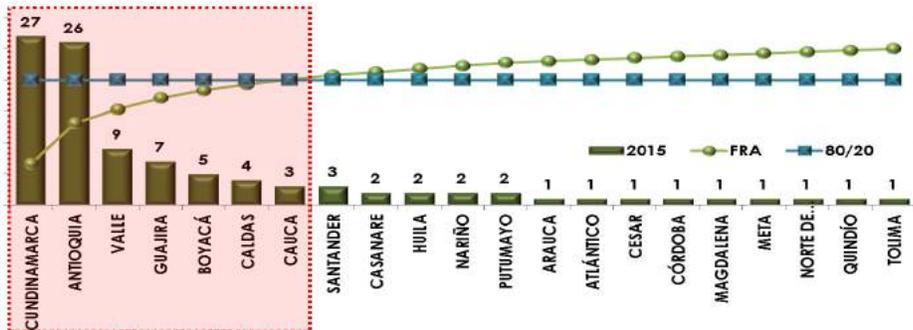
El mes de marzo con el 40% (40 casos)

es el de mayor registro, seguido de enero con el 11% (11) y junio y mayo con el 10% (10 hechos cada uno).

Los días domingos con un 40% (40 hechos) son los de mayor registro, seguido de los viernes con un 20% (20) y los miércoles con un 11% (11).

El 57% (58 hechos) fueron atendidos por la dirección de antinarcóticos, seguido de la regional Bogotá con un 20% (20) y la Dirección de Investigación Criminal e INTERPOL (DIJIN) con el 9% (9).

Gráfico 20. Departamentos con mayor registro de lavado de activos año 2015.

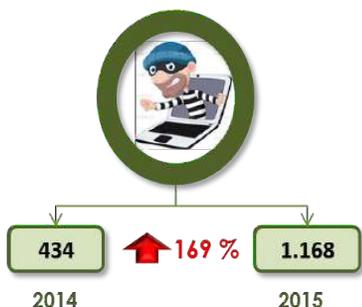


Fuente: SIEDCO

7 Departamentos concentran el 80% de lavado de activos, concentración estadística que debe motivar un análisis tendencial del riesgo.

Acceso abusivo a un sistema informático

Gráfico 21. Comparativo casos de acceso abusivo a un sistema informático años 2014-2015.



Fuente: SIEDCO

El 15% (171 casos) fueron perpetrados bajo la modalidad de ADWARE, seguido de SPOOFING y SPYWARE con el 4% (43 y 42 casos respetivamente), es de anotar que en 62% (720 hechos) no registran la modalidad.

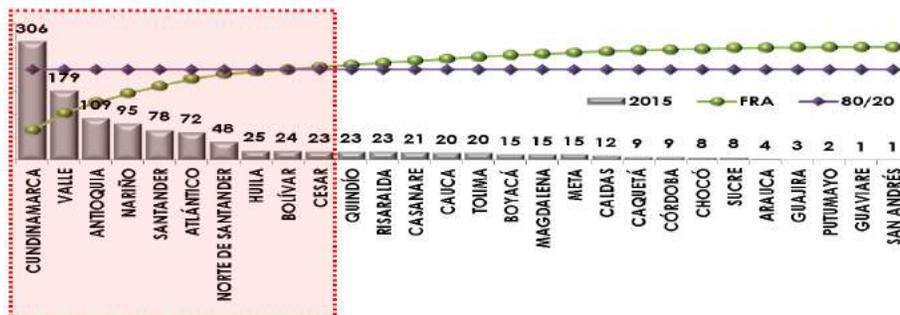
Los meses de agosto y octubre con el 10% (119 casos cada uno) son los de mayor registro, seguido de febrero y abril con el 9% (109 y 103 hechos respectivamente).

Las mujeres con el 67% (788 casos) son las más afectadas por este delito, mientras que en un 47% (548) fueron hombres.

Los días martes con un 19% (198 hechos) son los de mayor registro, seguido de los jueves, lunes y miércoles con el 15% (177, 176 y 174 hechos, respectivamente).

Los adultos con el 97% (1.128 casos) son los más afectados, seguido de los adolescentes con el 2% (76) y los menores con el 1% (13).

Gráfico 22. Departamentos con mayor registro de casos de acceso abusivo a un sistema informático año 2015.

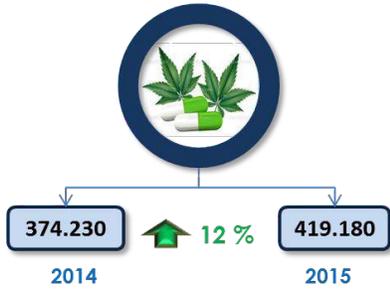


Fuente: SIEDCO

10 Departamentos concentran el 82% de casos de acceso abusivos a un sistema informático, razón por la cual debemos anticiparnos a las tendencias de cibercriminalidad mejorando las competencias profesionales.

Incautación de estupefacientes

Gráfico 23. Comparativo incautación de estupefacientes años 2014-2015.



Fuente: SIEDCO

La marihuana con el 52% (212.899 Kg) es el estupefaciente más incautado, seguido de la cocaína con el 40% (168.375 Kg), base de coca con el 8% (32.580 Kg) y el bazuco con el 1% (2.326).

El 71% (298.467 Kg) de estupefacientes fueron incautados en la zona rural,

mientras que en la urbana se incautó el 29% (120.713 Kg).

Capturas

Durante el 2015 se realizaron 75.361 capturas por tráfico, fabricación o porte de estupefacientes decremento del 12% en comparación con 2014 85.866.

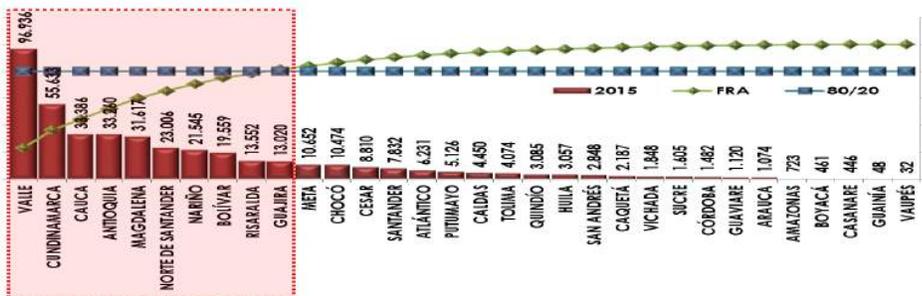
El 91% (68.219 capturas) fueron realizadas a hombres.

Tabla 1. Capturas estupefacientes 2014-2015.

CIRCUNSTANCIA CAPTURA	2014	2015
FLAGRANCIA LEY 906	80.665	69.834
ORDEN JUDICIAL LEY 906	4.889	5.225
ORDEN JUDICIAL LEY 600	312	302
TOTAL	85.866	75.361

Fuente: SIEDCO

Gráfico 24. Departamentos con mayor registro de casos de tráfico, fabricación o porte de estupefacientes año 2015.

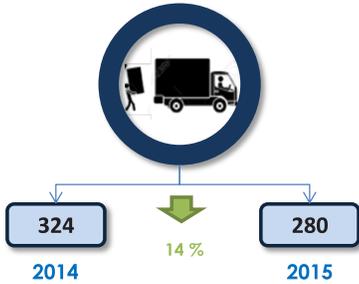


Fuente: SIEDCO

10 Departamentos concentran el 81% de incautación de estupefacientes, esto simboliza el esfuerzo focalizado de la sociedad civil y autoridades para reducir este flagelo.

Hurto de mercancías al transporte terrestre

Gráfico 25. Comparativo de hurto de mercancías, años 2014-2015.



Fuente: SIEDCO

Decremento del 14%, es decir (44 casos menos).

El 82% de los casos (230), fueron bajo la modalidad de atraco, seguido de violación de cerraduras con el 9% (24).

El arma de fuego se empleó en el 85% de los casos (237).

El 75% (209 casos) se realizaron en la zona rural.

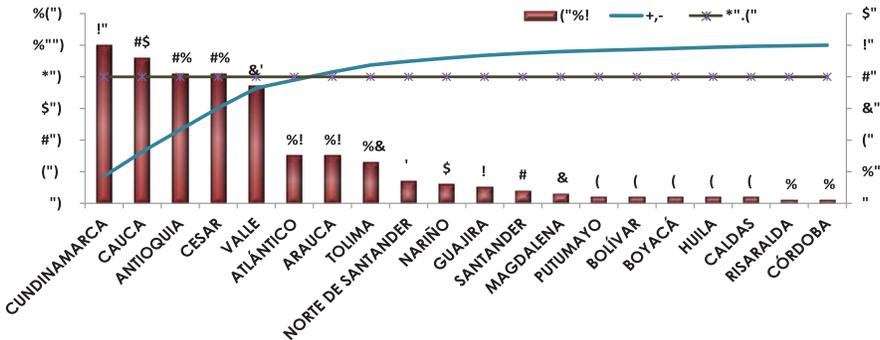
El mes de febrero con el 11%, es el mes de mayor participación, seguido de los meses de abril, marzo, enero y junio con el 10%.

Los días martes con el 21% (58 casos), registra mayor participación, le siguen los viernes con el 20% (56).

De 18:00 a 23:59 con el 30% (84 hechos), es la hora donde se más se registran casos, seguida de 06:00 a 11:59 con el 28% (77 casos).

Para el año 2015 se efectuaron 115 capturas, lo que representó un decremento del 3%, es decir (3 capturas menos).

Gráfico 26. Departamentos con mayor registro de hurto de mercancías, año 2015.



Fuente: SIEDCO

Estos 6 departamentos concentran el 80 % de la comisión de este delito con (230 hechos), análisis cuantitativo que debe motivar el trabajo conjunto de los diferentes actores de la cadena de suministro.

Hurto de mercancía en carreteras

Tipología número de casos 2015 - 2016



Bienes más hurtados



Viveres

1.309.867



Prendas

71.199



Repuestos

2.257



Combustible

1.309.867



Materiales

Construcción

43.765



Herramientas

43.765

Fuente: SIEDCO Periodo del 01/01/2015 al 31/08/2015 del 01/01/2016 al 31/08/2016

Otras variables de análisis para el hurto de mercancía en carreteras

Casos hurto de mercancía

Del 01 de enero al 20 de Agosto

2015	2016	Total	Dif.	%
206	191	377	-35	-35

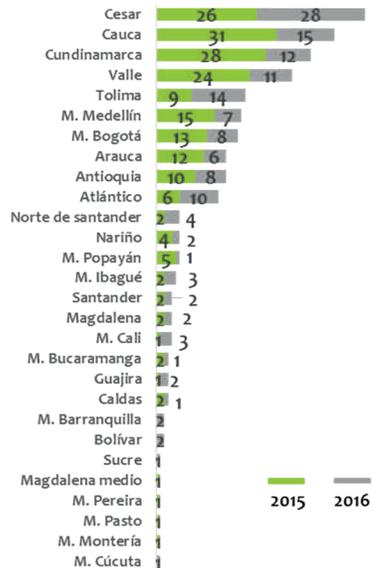
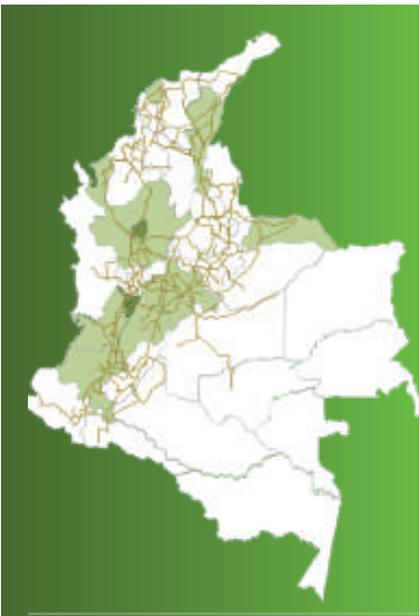
Hurto por zona

	2015	2016	Dif.	%
Rural	156	134	-22	14
Urbana	50	37	-13	-26
Total	206	171	-35	-17

Meses de mayor afectación



Unidades con mayor afectación



1.5.3 Desde uno de los Sistemas de Gestión certificados por el sector privado (hallazgos frecuentes)

Ficha técnica



Estadísticas de no conformidades (hallazgos)
Frente a la Norma BASC versión 04 de 2.012



Fuente: WORLD BASC ORGANIZATION – BASC
Colombia - Bogotá.



Muestra: 127 Auditorías Externas realizadas entre
enero 1° a agosto 31 de 2016 (1.016 horas de
auditoría) en todos los sectores económicos de la
cadena de suministro global.

NUMERAL, NORMA DE SEGURIDAD BASC: 4.4.6

CANTIDAD
DE
HALLAZGOS
28

Descripción del estándar

Control Operacional

La organización debe asegurar, con base en su evaluación de riesgos, responsabilidad y participación en la cadena de suministro y las actividades relacionadas con el comercio internacional, que los planes, programas y controles de seguridad se encuentran totalmente integrados en todo el ámbito de la organización y dentro de todas sus actividades. Al implementar la política y la gestión efectiva del control y la seguridad, la organización debe hacer lo necesario para garantizar que todas las actividades se realicen de manera segura.

Descripción de la no conformidad

Falta de trazabilidad, control, seguimiento y registros que permitan demostrar el aseguramiento las operaciones.

NUMERAL, NORMA DE SEGURIDAD BASC: 4.3.4

CANTIDAD DE HALLAZGOS
21

<p>Descripción del estándar</p>	<p>Requisitos Legales y de otra índole La organización debe tener un procedimiento documentado para identificar, actualizar, implementar y comunicar los requisitos legales y reglamentarios al cual esté sometido y le sea aplicable al SGCS BASC. La organización debe asegurar el cumplimiento de las disposiciones y normas relativas a proteger la propiedad intelectual, incluyendo la propiedad de Norma y Estándares BASC y el uso adecuado del logo que identifica la marca y la imagen corporativa de WBO.</p>
<p>Descripción de la no conformidad</p>	<p>Incumplimiento legal frente a:</p> <ul style="list-style-type: none"> - Credenciales de personal de seguridad vencidas. - Sistema Sarlaft. - Circular 170 de la DIAN. - Decreto 1377 de 2013. - Decreto 1539 Examen psicofísico. - No identificación de aplicación de requisitos legales.

NUMERAL, NORMA DE SEGURIDAD BASC: 4.5.2

CANTIDAD DE HALLAZGOS
16

<p>Descripción del estándar</p>	<p>Auditoría La organización debe tener un procedimiento documentado para realizar auditorías internas a los elementos del SGCS con el fin de verificar que esté conforme con:</p> <p>a) Los requisitos de la Norma y los Estándares de seguridad BASC.</p> <p>b) Los requisitos del Sistema de Gestión en Control y Seguridad establecidos e implementados por la organización.</p> <p>La organización debe elaborar y ejecutar un programa de auditorías internas, su enfoque y periodicidad debe ajustarse a la madurez del SGCS, resultados de auditorías anteriores, importancia y criticidad de los procesos identificada en el análisis y evaluación de riesgos con una frecuencia mínima de una vez al año. Las auditorías internas al SGCS BASC, deben ser realizadas por un equipo de auditores competentes, independientes a los procesos auditados, formados a través de los capítulos BASC por instructores aprobados por WBO. Estos Auditores Internos deberían ser propios de la organización, con el fin de garantizar la continuidad del SGCS y el seguimiento de los resultados obtenidos en los procesos de</p>
--	---





	<p>auditoría. Los auditores internos deben ser capacitados y entrenados en temas relacionados con auditorías de sistemas de gestión y seguridad de la cadena de suministro y reentrenados cuando existan cambios procedimentales o normativos en WBO.</p>
<p>Descripción de la no conformidad</p>	<p>No se cuenta con programa de auditorías, ni un plan de auditorías No hay registros de auditoría que garanticen la revisión del 100% de los requisitos. No se realizan auditorías internas al sistema de gestión en control y seguridad No se cuenta con el equipo de auditores competente.</p>

NUMERAL, NORMA DE SEGURIDAD BASC: 4.6.2

CANTIDAD DE HALLAZGOS
16

<p>Descripción del estándar</p>	<p>Acción Correctiva y Preventiva La organización debe tener procedimientos documentados para la implementación de acciones correctivas y preventivas, los cuales deben ser aplicados cuando se evidencien no conformidades reales o potenciales en el SGCS, teniendo en cuenta los siguientes aspectos: a) Revisar las desviaciones del SGCS. b) Identificar la causa de las situaciones no conformes. c) Identificar y aplicar las medidas pertinentes. d) Registrar las acciones preventivas o correctivas. e) Verificar la eficacia de las acciones tomadas</p>
<p>Descripción de la no conformidad</p>	<p>No se realizan análisis de causas adecuados, no se llega a la causa raíz. No se efectúan los tratamientos correspondientes. No se hace seguimiento a las acciones planteadas para realizar los cierres de no conformidades. No se aplica lo determinado en los procedimientos de acciones correctivas, preventivas y mejora No se diferencian las correcciones de las acciones correctivas.</p>

NUMERAL, NORMA DE SEGURIDAD BASC: 4.3.3**CANTIDAD DE
HALLAZGOS
12**

Descripción del estándar	<p>Gestión del Riesgo</p> <p>La organización debe tener un procedimiento documentado para establecer e implementar un proceso de gestión de riesgos que permita la determinación del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos. Debe realizar una reevaluación de los riesgos mínimo una vez al año y/o cuando se identifiquen nuevas amenazas o vulnerabilidades en el SGCS.</p>
Descripción de la no conformidad	<p>No se aplica adecuadamente la metodología de gestión de riesgos.</p> <p>No se identifican todos los riesgos relacionados con la cadena de suministro</p> <p>No se actualizan los riesgos, ni se dejan registros de las revisiones.</p>

NUMERAL, NORMA DE SEGURIDAD BASC: 4.6.3**CANTIDAD DE
HALLAZGOS
8**

Descripción del estándar	<p>Compromiso de la Dirección</p> <p>La Alta Dirección debe realizar a intervalos planificados, mínimo una vez al año, revisiones del SGCS BASC y debe considerar el análisis de los siguientes aspectos:</p> <ul style="list-style-type: none"> a) Desempeño global del sistema. b) Desempeño individual de los procesos del SGCS. c) Resultados de las auditorías. d) Resultados de las acciones preventivas, correctivas y de mejora. e) Cambios que puedan afectar el SGCS. f) Resultados de la gestión de riesgos. g) Revisiones anteriores. <p>World La revisión debe estar documentada contemplando las instrucciones y lineamientos gerenciales para asegurar la eficacia del SGCS y la coherencia con las proyecciones estratégicas. Como resultado de la revisión por la Alta Dirección se debe evidenciar la toma de decisiones y asignación de recursos para el cumplimiento de la Política de Control y Seguridad.</p>
Descripción de la no conformidad	<p>La revisión por la dirección no mide el desempeño y la eficacia de los procesos, ni documenta, argumenta y concluye sobre los procesos.</p> <p>La revisión por la dirección no documenta y/o argumenta la conformidad.</p>

NUMERAL, NORMA DE SEGURIDAD BASC: 4.4.7**CANTIDAD DE
HALLAZGOS**
8**Descripción del
estándar****Preparación y Respuesta a Eventos Críticos**

La organización debe tener procedimientos documentados para:

- a) Identificar y responder oportunamente ante amenazas y vulnerabilidades.
- b) Responder oportunamente ante situaciones críticas, para mitigar el impacto y el efecto que estos eventos o situaciones puedan generar sobre las operaciones o la imagen de la organización mediante procedimientos de contingencia y emergencia.
- c) Realizar ejercicios prácticos y simulacros que prueben la eficacia de las medidas de protección, así como las medidas previstas para dar respuesta a eventos críticos.
- d) Investigar todos aquellos elementos del sistema que tuvieron relación, directa o indirecta, con la falla presentada. Nota: La respuesta a eventos críticos, debe estar sujeta a la gestión de riesgos a través de planes de contingencia y emergencia.

**Descripción de la no
conformidad**

No se cuenta con suficientes planes de contingencia.
No se realizan simulacros al sistema de gestión en control y seguridad.

NUMERAL, NORMA DE SEGURIDAD BASC: 4.3.2**CANTIDAD DE
HALLAZGOS**
4**Descripción del
estándar****Objetivos del SGCS**

La Alta Dirección debe establecer y revisar los objetivos del SGCS en las funciones y los niveles pertinentes dentro de la organización. Dichos objetivos deben ser coherentes y permitir dar evidencia del cumplimiento de la política de control y seguridad a través de indicadores de gestión.

**Descripción de la no
conformidad**

No se establecen y revisan los objetivos en las funciones y niveles pertinentes
No son coherentes los objetivos y no permiten evidenciar el cumplimiento de la política.

NUMERAL, NORMA DE SEGURIDAD BASC: 4.4.5

CANTIDAD DE HALLAZGOS
4

Descripción del estándar

Control de Documentos

La organización debe tener un procedimiento documentado que incluyan listados maestros de documentos que le permitan controlar todos los documentos requeridos para la implementación del SGCS BASC, y garantizar que:

- a) Se aprueben los documentos antes de su emisión.
- b) Puedan ser localizados oportunamente.
- c) Se revisen periódicamente y se actualicen cuando sea necesario.
- d) Se encuentren legibles y disponibles garantizando su preservación, custodia y confidencialidad.
- e) Sean oportunamente identificados y retirados los documentos obsoletos para evitar su uso no previsto; incluyendo aquellos que deban ser retenidos con propósitos de preservación legal o de conocimiento.
- f) Se controlen los documentos de origen externo.
- g) Se disponga de un sistema de protección y recuperación de la información sensible de la organización que incluya medios magnéticos y físicos.

Descripción de la no conformidad

Falta control de los documentos y se garantice la emisión, localización, revisión, actualización y su disponibilidad.

NUMERAL, NORMA DE SEGURIDAD BASC: 4.4.2

CANTIDAD DE HALLAZGOS
3

Descripción del estándar

Entrenamiento, Capacitación y Toma de Conciencia

La organización debe determinar y demostrar las competencias requeridas del personal y en caso de no disponer de ellas, debe tomar las acciones necesarias. El personal debe ser consciente de la responsabilidad por el control y seguridad en todos los niveles de la organización y de la influencia que su acción o inacción pueda tener sobre la eficacia del SGCS BASC.

Descripción de la no conformidad

No se determina y demuestra la competencia del personal.

NUMERAL, NORMA DE SEGURIDAD BASC: 1.2**CANTIDAD DE
HALLAZGOS**
2

97

Descripción del estándar	<p>Para usar esta Norma</p> <p>Los requisitos contemplados en esta Norma son todos esenciales para la implementación de un Sistema eficaz de Gestión de Control y Seguridad y se complementan de manera directa con Estándares Internacionales de Seguridad BASC – C-TPAT creados para los distintos sectores partícipes en la cadena de suministro y las actividades relacionadas con el comercio internacional. Los factores humanos, incluyendo la cultura, políticas, etc., dentro de las organizaciones, pueden crear o destruir la efectividad de cualquier sistema de gestión y se deben considerar cuidadosamente al implementar esta Norma. Siguiendo cada etapa, las organizaciones podrán establecer procedimientos para determinar la política y objetivos de seguridad, al igual que procedimientos para su implementación y demostrar sus logros según criterios definidos. Las organizaciones deben tener en cuenta que para la implementación de su SGCS priman los requisitos de orden legal aplicables en el país donde la organización tiene sede, sobre los criterios de norma y estándares; por tanto, ningún requisito puede implementarse incumpliendo la normatividad legal vigente de cada país. Las organizaciones deben demostrar que cumplen los requisitos legales, antes de buscar la conformidad y el mejoramiento continuo del SGCS.</p>
Descripción de la no conformidad	No se demuestra el cumplimiento de los requisitos legales, antes de buscar la conformidad del SGCS.

NUMERAL, NORMA DE SEGURIDAD BASC: 4.5.1**CANTIDAD DE
HALLAZGOS**
2

Descripción del estándar	<p>Seguimiento y Medición</p> <p>La organización debe tener procedimientos documentados para el seguimiento y medición de las características claves que puedan tener impacto significativo en el control y seguridad y se debe ajustar a las necesidades de la organización, estableciendo indicadores y metas que permitan determinar la eficacia del SGCS BASC.</p>
Descripción de la no conformidad	No se llevan a cabo el seguimiento, mediciones acordes con las necesidades de la Organización a través de indicadores que midan la eficacia del SGCS.

NUMERAL, NORMA DE SEGURIDAD BASC: 1.3

CANTIDAD DE HALLAZGOS
1

Descripción del estándar	<p>Aplicación Todos los requisitos de esta Norma Internacional son genéricos y aplicables a todas las organizaciones elegibles, sin importar su tipo o tamaño. El alcance de su aplicación depende del objeto social (giro del negocio), los riesgos presentes en la cadena de suministro, las actividades relacionadas con el comercio internacional y las condiciones del entorno en el cual opera. Cuando uno o varios requisitos consignados en los Estándares de Seguridad no se puedan aplicar debido a la naturaleza de la organización pueden excluirse siempre y cuando estén debidamente justificados y documentados.</p>
Descripción de la no conformidad	<p>No es claro el alcance de la certificación por parte de la Organización.</p>

NUMERAL, NORMA DE SEGURIDAD BASC: 4.2.5

CANTIDAD DE HALLAZGOS
1

Descripción del estándar	<p>Seguridad del Personal propio, subcontratado y suministrado Debe contar con un programa de concientización sobre adicciones al alcohol, drogas, juego, entre otras adicciones, que incluya avisos visibles y material de lectura.</p>
Descripción de la no conformidad	<p>No se cuenta con un programa de concientización sobre adicciones al alcohol.</p>

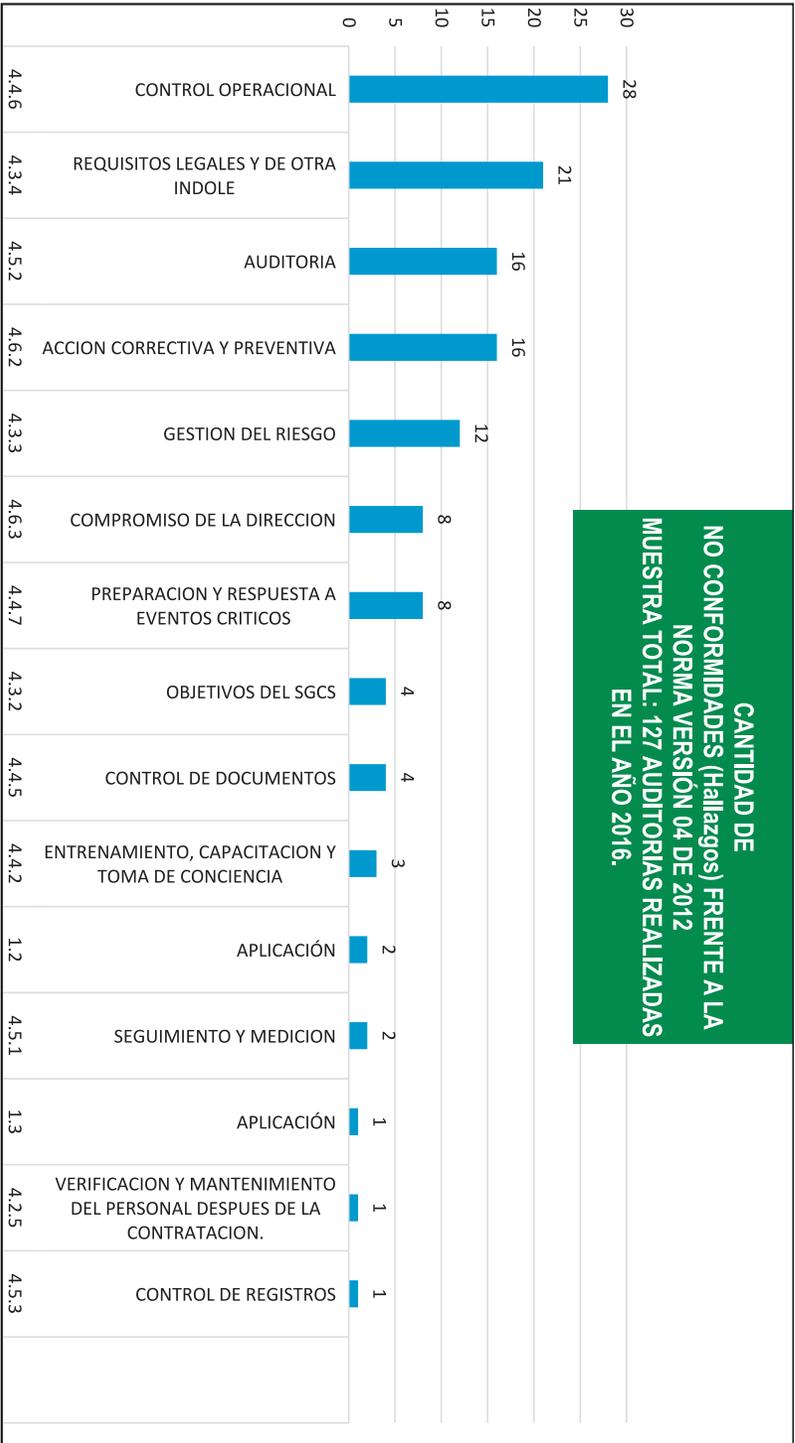
NUMERAL, NORMA DE SEGURIDAD BASC: 4.5.3**CANTIDAD DE
HALLAZGOS****99****1****Descripción del
estándar****Control de Registros**

La organización debe llevar los registros necesarios para demostrar conformidad con los requisitos del SGCS BASC y tener un procedimiento documentado, que incluya listado maestro de registros, para la identificación, mantenimiento, disposición de estos registros y para la entrega, control y archivo de la información, teniendo en cuenta los tiempos de conservación previstos en la legislación y definidos por las necesidades de la organización. Los registros deben ser legibles, identificables y rastreables de acuerdo con la actividad, producto o servicio involucrado y se deben almacenar en un lugar adecuado y seguro de forma que se puedan recuperar fácilmente y proteger contra daños, deterioro, pérdida o alteración.

**Descripción de la no
conformidad**

Los registros no son fáciles de ubicar.

“Los sistemas de control y seguridad permiten a las empresas asegurar procesos y procedimientos para interactuar en una cadena de valor, con mayor confianza”.



Ficha técnica

Estadísticas de no conformidades (hallazgos)
Frente a los estándares de seguridad BASC versión 04 de 2.012



Fuente: WORLD BASC ORGANIZATION – BASC
Colombia - Bogotá.



Muestra: 97 Auditorías Externas realizadas entre Enero 1° a Agosto 31 de 2016 (776 horas de auditoría) en todos los sectores económicos de la cadena de suministro global.

NUMERAL, ESTANDAR DE SEGURIDAD: 1.1.1

**CANTIDAD DE
HALLAZGOS**
23

Descripción del estándar

Deben existir procedimientos documentados y verificables para la selección de sus asociados de negocio (clientes, proveedores y terceras partes) vinculadas en la cadena de suministro, que contemplen parámetros más allá de los requisitos financieros, incluyendo indicadores de seguridad.

Descripción de la no conformidad

No se verifica la selección de los asociados de negocio que contemplen parámetros más allá de los requisitos financieros.

NUMERAL, ESTANDAR DE SEGURIDAD: 1.2

**CANTIDAD DE
HALLAZGOS**
18

Descripción del estándar

Debe asegurar que los Asociados de Negocio desarrollen procesos y procedimientos de seguridad compatibles con el SGCS BASC, con el fin de mantener la integridad de la carga desde el punto de origen hasta el punto de destino. Debería realizar verificaciones periódicas de los procesos e instalaciones de los Asociados de Negocio basado en un proceso de gestión del riesgo y estos deberían mantener las normas de seguridad requeridas por el exportador.

Descripción de la no conformidad

No se aplican procesos de selección y evaluación de asociados de negocio con criterios de prevención contra el lavado de activos y financiación del terrorismo.

NUMERAL, ESTANDAR DE SEGURIDAD: 4.1.3

Descripción del estándar	Debe realizar, de conformidad con la legislación local, una visita domiciliaria al personal que ocupará las posiciones críticas o que afecta a la seguridad, antes de que ocupe el cargo y actualizarla cada dos años.
Descripción de la no conformidad	No se realizan las visitas domiciliarias a todo el personal de posiciones críticas.

CANTIDAD DE HALLAZGOS
16

NUMERAL, ESTANDAR DE SEGURIDAD: 2.5.3

Descripción del estándar	Debe tener procedimientos para reconocer y reportar a las autoridades aduaneras o la autoridad pertinente, cuando los sellos, contenedores o furgones han sido comprometidos.
Descripción de la no conformidad	No se cuenta con el procedimiento para reportar cuando los sellos, contenedor o furgón han sido comprometidos.

CANTIDAD DE HALLAZGOS
13

NUMERAL, ESTANDAR DE SEGURIDAD: 7.1.1

Descripción del estándar	Debe asignar cuentas individuales que exijan un cambio periódico de la contraseña para los sistemas automatizados
Descripción de la no conformidad	No se asignan cuentas individuales con cambio periódico para los sistemas automatizados.

CANTIDAD DE HALLAZGOS
4

NUMERAL, ESTANDAR DE SEGURIDAD: 1.1.4

Descripción del estándar	Debe establecer por escrito acuerdos de seguridad para aquellos Asociados de Negocio que no estén certificados por BASC, que describan el cumplimiento de los criterios de Seguridad BASC que hayan sido establecidos como resultado de la evaluación de riesgos.
Descripción de la no conformidad	No se establecen acuerdos de seguridad como resultado de la evaluación de riesgos.

CANTIDAD DE HALLAZGOS
3

NUMERAL, ESTANDAR DE SEGURIDAD: 1.1.5		CANTIDAD DE HALLAZGOS 3
Descripción del estándar	Debe verificar los procedimientos de seguridad que ha implementado el Asociado de Negocio No BASC, basándose en un proceso documentado de gestión de riesgos.	
Descripción de la no conformidad	No se verifican los procedimientos de asociados de negocios no BASC, basados en un proceso de gestión del riesgo.	
NUMERAL, ESTANDAR DE SEGURIDAD: 5.4.4		CANTIDAD DE HALLAZGOS 3
Descripción del estándar	Debe contar con procedimientos documentados para el manejo y control de materias primas	
Descripción de la no conformidad	No se garantiza el manejo y control de materias primas y material de empaque.	
NUMERAL, ESTANDAR DE SEGURIDAD: 2.1.1		CANTIDAD DE HALLAZGOS 4
Descripción del estándar	Debe mantener la integridad de los contenedores, furgones, remolques y la carga para protegerlos contra la introducción de materiales y personas no autorizadas.	
Descripción de la no conformidad	No se mantiene la integridad del contenedor, furgones remolques y carga.	
NUMERAL, ESTANDAR DE SEGURIDAD: 4		CANTIDAD DE HALLAZGOS 2
Descripción del estándar	Requisitos del sistema de gestión en control y seguridad (SGCS) BASC	
Descripción de la no conformidad	No se evalúa a los candidatos con posibilidad de contratación, ni se realizan verificaciones periódicas.	

NUMERAL, ESTANDAR DE SEGURIDAD: 8

Descripción del estándar	Entrenamiento de seguridad y concientización sobre amenazas.
Descripción de la no conformidad	No se cuenta con un programa anual de capacitación que garantice la competencia en el reporte de amenazas y vulnerabilidades.

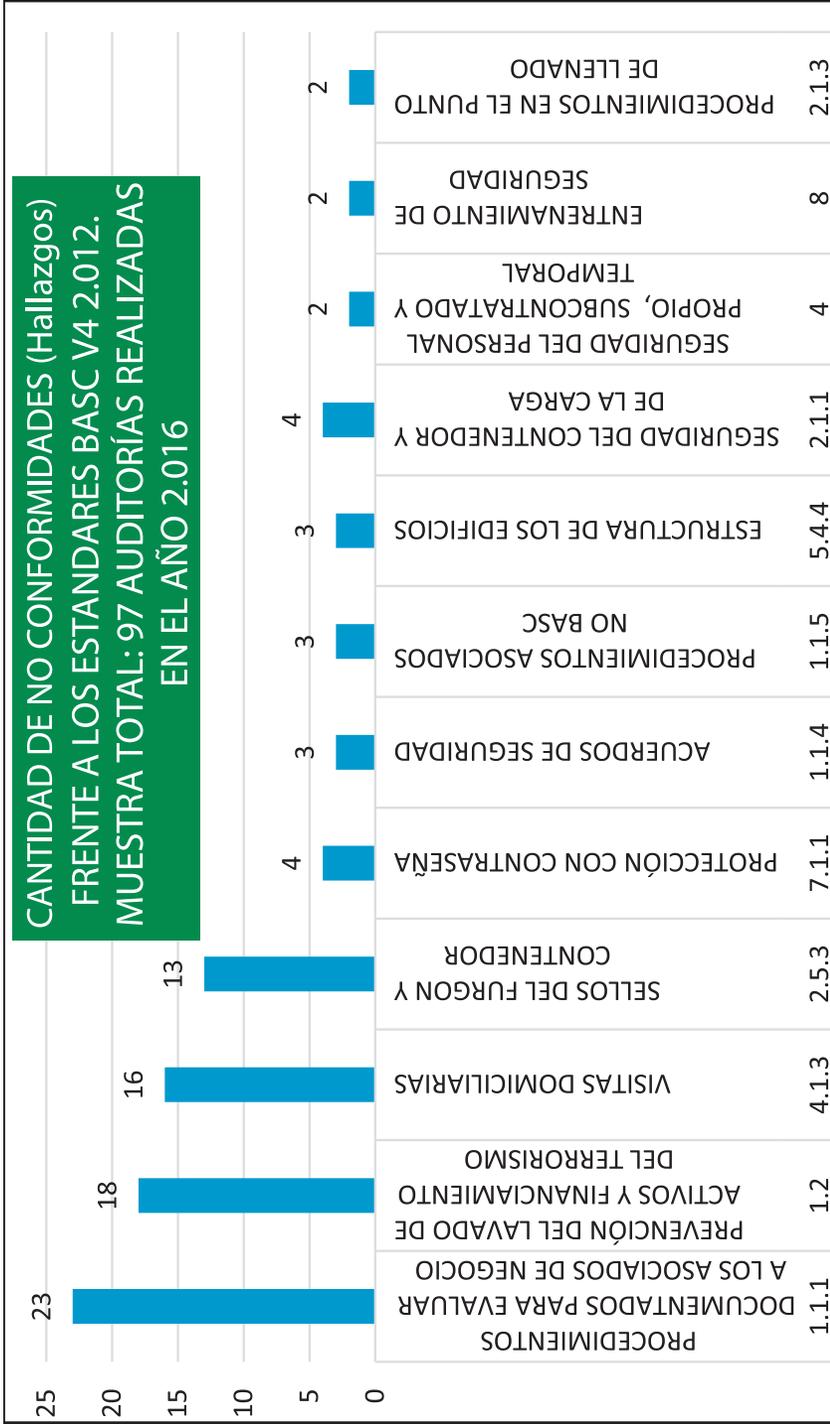
CANTIDAD DE HALLAZGOS
2

NUMERAL, ESTANDAR DE SEGURIDAD: 2.1.3

Descripción del estándar	Debe tener procedimiento documentos en el punto de llenado para sellar correctamente y mantener la integridad de los contenedores y furgones.
Descripción de la no conformidad	No se garantiza en el punto de llenado, el cierre y la integridad de los contenedores.

CANTIDAD DE HALLAZGOS
2

“Pertener al Frente de Seguridad Empresarial de la DIJIN, aporta al mantenimiento de un sistema de control y seguridad en la empresa, toda vez que se accede a oportunidades de mejora continua en la trazabilidad de la cadena de suministro y se logra la disminución de pérdidas económicas”.



Miguel Velásquez Olea, Director Ejecutivo BASC Bogotá – Colombia

1.6 Aproximación prospectiva de riesgos sociales y criminales de atención empresarial



“Los problemas globales requieren una ética global que reconozca los valores locales, por lo que es importante reconocer el riesgo en un contexto de creciente incertidumbre

Gutiérrez, Miguel Ángel, “Hacia un Análisis de los Riesgos Globales”



El crecimiento económico y desarrollo social está asociado al principio de confianza del consumidor y los inversionistas; el propósito es cerrar brechas entre las vulnerabilidades que generan las amenazas globales y los riesgos sociales, los cuales generan incertidumbre; estado indefectible que expone a un país a la desventaja competitiva global, dada la interacción de las cadenas de valor como locomotoras de progreso y de acuerdo con la dinámica de un intercambio de productos y servicios cuyos estándares son cada vez más exigentes en calidad, innovación, el uso de la tecnología para reducir costos, en oportunidad y sobre todo en **seguridad**.

La seguridad está en la agenda de todo el mundo. Esta conciencia colectiva es la que ha permitido que hoy tengamos, pese a la tendencia hemisférica y regional, un país que busca una paz con seguridad sostenible e integral; a pesar de su historia y su entorno de seguridad actual, hoy logramos en favor de Colombia, tener apreciaciones como las del Fondo Monetario Internacional FMI, el cual en su examen anual considera que **“la economía colombiana es resistente y sólida frente a los choques externos”**, dadas las garantías y esfuerzos en materia de seguridad, las cuales han permitido generar mayor confianza para la inversión extranjera y la continuidad de los negocios. Así lo ratifican compromisos vigentes, como la alianza del pacífico, el Operador Económico Autorizado OEA, los informes de aportes de cada país a los 17 objetivos de desarrollo sostenible y su alineación con el Plan Nacional de Desarrollo, los cuales otorgan un lugar privilegiado a las garantías de seguridad y justicia, más aún si se analizan los dividendos para la paz.

Debido a este contexto, el futuro de Colombia marca una construcción en torno al goce de garantías de convivencia y seguridad ciudadana en el marco de un posacuerdo; esta ya es una prioridad del Estado colombiano, derecho que involucra también a los empresarios en el país, cuando se trata de identificar los riesgos sociales y criminales para asegurar su negocio y su cadena de suministro. En la práctica, la seguridad

empresarial estará marcada por una visión integral del riesgo, que privilegie la prevención criminal y el desarrollo de la capacidad de resiliencia, lo cual permitirá una mayor adaptación.

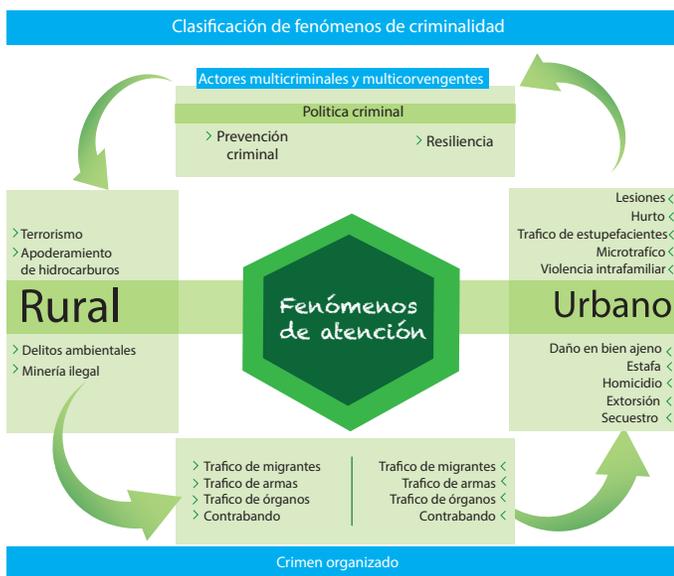
Generar la transición implica reconocer diferentes escenarios, pero sobre todo el más probable, el cual está relacionado con tener una visión muy práctica, pero asertiva para asumir los retos y desafíos de la seguridad, en un escenario que estará caracterizado por fenómenos emergentes, quizás otros que cambiarán u otros que se agudizarán. En este sentido, aquí encontrará para minimizar la incertidumbre algunos fenómenos de referencia que podrían ser analizados para asesorar la toma de decisiones, con el fin de superar barreras y actualizar el panorama de riesgo de acuerdo con su negocio.

Factores de atención institucional y empresarial:

1. Incremento de la protesta social: Nuevas formas de manifestación, exacerbación de otros derechos (bloqueo de economías, infiltración, inclusión).
2. Conflictos sociales: pandillismo, vandalismo, lesiones personales.
3. Violencia contra poblaciones especiales: grupos identitarios (guardias indígenas, poblaciones vulnerables).
4. Intolerancia social: riñas, problemas de vecindad.
5. Crecimiento demográfico – urbanización: asentamientos colectivos.
6. Necesidades básicas insatisfechas (salud, educación y servicios públicos), desempleo, seguridad alimentaria.
7. Cultura de ilegalidad: gota a gota, mototaxismo, anomia social, cultura del atajo social, cumplimiento medidas Código Nacional de Policía.
8. Índice de violencias: violencia política (Apertura democrática), intrafamiliar, contra la mujer y los niños y adolescentes, ajuste de cuentas, cifras de homicidios.
9. Justicia transicional: víctimas, desmovilización, reinserción y memoria histórica.
10. Insostenibilidad del capital ambiental: cambios climáticos y delitos ambientales.
11. Riesgos sociales: indigencia, basuras, despenalización del consumo drogas, enfermedades, delitos que afectan el patrimonio económico de las personas (hurto), influencia en adicciones populares, prostitución, consumo de alcohol, pérdida de valores.
12. Nuevas formas de gestión organizacional y territorial, reingenierías institucionales.

Riesgos de criminalidad de atención institucional y empresarial

1. Reincidencia criminal.
2. Mutación del crimen a empresas criminales (glocalización).
3. Actores multictiminales y multiconvergentes (negociación de rentas criminales)
4. Corrupción
5. Delitos transnacionales (desalineación política criminal).
6. Ciber-criminalidad: (Por desarrollo tecnológico, uso de las redes, cambios tecnológicos, big data).
7. Sostenibilidad del narcotráfico: Pasó de ser productores a incremento del consumo de estupefacientes en la población colombiana – problema de salud pública y tendencia mundial de despenalización.
8. Extorsión de menor cuantía a segmentos de la población (nuevos modelos de economías criminales y de escala).
9. Delitos que afectan el patrimonio económico de las personas.
10. Identificación del crimen organizado, así como grupos emergentes, tanto en lo urbano como en lo rural, que implicarán una política criminal más sólida, si se considera la siguiente clasificación:



Teniendo en cuenta esta perspectiva, diagnosticar metodológicamente el futuro de su negocio en un escenario ideal, indeseable y probable, le permitirá establecer una metavisión de su negocio y construir un futuro sostenible, debido a que ha previsto factores que le permitirán minimizar ser víctima y asegurar su evolución a partir de un claro mapa de riesgos sociales y criminales y sobre todo del fortalecimiento del trabajo conjunto con las autoridades.

Mayor Gelga Buitrago Martínez

Jefe Área Asistencia y Cooperación para la Policía Judicial, Frentes de Seguridad Empresarial

2

CAPÍTULO



Buenas prácticas,
lecciones aprendidas
y recomendaciones

2. BUENAS PRÁCTICAS, LECCIONES APRENDIDAS Y RECOMENDACIONES

2.1 El desarrollo de competencias del líder de seguridad en cadena de suministro



Acorde con los estándares de seguridad que emite la Organización Internacional de Normalización, ISO

Las competencias en una persona son aquellos conocimientos, habilidades, destrezas, comportamiento y experiencia que le permite desarrollar una actividad de manera eficaz y eficiente en su vida laboral.

¿Qué relación guardan las competencias de una persona con los estándares que emite la Organización Internacional de Normalización, ISO, la cual fue fundada el 23 de febrero de 1947 por 196 países para la creación de estándares en muy diversas áreas para su aplicación a nivel mundial?

Desde hace décadas los profesionales y líderes de la seguridad han encontrado en los estándares ISO el aliado perfecto para implementar en sus organizaciones, tanto públicas como privadas, un sistema de gestión de seguridad robusto creando procesos específicos con enfoque preventivo, ante una gran diversidad de riesgos y amenazas que está expuesta toda organización.

En el contexto del comercio internacional es evidente que para los países es indispensable que las cadenas de suministro de cada uno deberán desarrollar una movilización fluida de millones de toneladas de bienes y materiales, que se comercializan todos los días a través de una cadena logística integrada, principalmente, por empresas de manufactura, transporte de carga terrestre, marítima, aérea, ferroviaria, agencias aduanales, recintos fiscalizados, operadores logísticos, agentes navieros, entre otros. Si estos procesos logísticos se ven alterados o interrumpidos a causa de eventos, tales como sabotaje, robo, asaltos, accidentes, daños a la infraestructura, siniestros, fraudes y un sinnúmero de afectaciones, el impacto sobre el flujo de bienes es incalculable. Por lo tanto, el líder de seguridad de hoy en día, responsable de gestionar estos riesgos para garantizar la continuidad de operaciones críticas, requiere de cada vez mejores herramientas de carácter global; además, de sumar a sus responsabilidades la correcta gestión de programas de certificación de seguridad en cadena de suministro como es el

caso del Customs Trade Partnership Against Terrorism, CTPAT, y el Operador Económico Autorizado de la Organización Mundial de Aduanas.

Ante este escenario, en la Organización Internacional de Normalización, ISO, entró en funcionamiento el 1° de enero de 2015, creando un nuevo comité internacional con el numeral ISO/TC 292 denominado "Security and Resilience".

Acerca del Comité Técnico Internacional ISO TC/292 – Security and Resilience / Seguridad y Resiliencia.

La responsabilidad del Comité Técnico ISO/TC 292 está a cargo del Instituto de Normas de Suecia, SIS. La autoridad sueca de protección civil apoya el desarrollo de normas de la especialidad elaboradas por un organismo internacional, debido a que se las considera herramientas de consenso con todos los representantes sociales, muy importantes para una comunidad participativa y más segura.

Este nuevo Comité Técnico ISO/TC 292 para la seguridad y resiliencia fue creado con el propósito de incrementar la seguridad de la sociedad ante incidentes perjudiciales, emergencias y desastres causados por actos humanos intencionales y accidentales, amenazas, desastres naturales y daños a la infraestructura.

Actividad del Comité Técnico ISO/TC 292 Seguridad y resiliencia.

Las normas ISO que sirven a la Seguridad de la Sociedad y a la Resiliencia, están diseñadas como herramientas para todo tipo de organización, independientemente de su actividad; prioriza la capacitación profesional y hace más efectiva la prevención, respuesta, recuperación ante emergencias y desastres de cualquier naturaleza. De este modo, contribuyen también al desarrollo del mercado para la provisión de bienes y servicios locales, que sirvan para una más eficiente coordinación de los esfuerzos nacionales e internacionales para responder a emergencias y desastres que aseguren la continuidad de las operaciones y negocios en todos los ámbitos posibles.

El Comité Técnico ISO/TC 292 Seguridad y Resiliencia está conformado por una estructura de 5 grupos específicos (Importante: Se respeta el nombre oficial con el que ISO las ha clasificado y /o publicado).

LISTADO 1: Continuity and resilience

LISTADO 2: Emergency management and public and community resilience

LISTADO 3: Private security services and operations

LISTADO 4: Supply Chain and security management

LISTADO 5: Corruption, Fraud, and Counterfeiting

LISTADO 1

- ISO 22300:** 2012 Societal security
 - Terminology
- ISO 22301:**2012 Societal security
 - Business continuity management systems
 - Requirements
- ISO 22311:** 2012 Societal security
 - Video - surveillance
 - Export interoperability
- ISO/TR 22312:** 2011 Societal security
 - Technological capabilities
- ISO 22313:** 2012 Societal security
 - Business continuity management systems
 - Guidance
- ISO 22316*** Societal security
 - Organizational resilience
 - Principles and guidelines
- ISO 22317*** Societal security
 - Business continuity management systems
 - Business impact analysis (BIA)
- ISO 22318*** Societal Security
 - Business continuity management systems
 - Guidance for supply chain continuity management systems

LISTADO 2

- ISO 22315:**2014 Societal security
 - Mass evacuation
 - Guidelines for planning
- ISO 22320:** 2011 Societal security
 - Emergency management
 - Requirements for incident
- ISO 22324:**2015 Societal security
 - Emergency management
 - Guidelines for colour-coded
- ISO 22397:**2014 Societal security
 - Guidelines for establishing partnering arrangements

- ISO 22398:** 2013 Societal security
 - Guidelines for exercises
- ISO 22319*** Societal security
 - Guidance for involving volunteers in the response to major incidents
- ISO 22325*** Societal security
 - Emergency management
 - Guidelines for emergency
- ISO 22326*** Societal security
 - Emergency management
 - Guidance for monitoring of ISO/TR 22351* Societal security
 - Emergency management
 - Message structure for exchange
- ISO 22322*** Societal security
 - Emergency management
 - Guidelines for public warning

LISTADO 3

- ISO 18788***
 - Management system for private security operations
 - Requirements with guidance terminology

LISTADO 4

- ISO 28000:** 2007 Specification for security management systems for the supply chain
- ISO 28001:** 2007 Security management systems for the supply chain
 - Best practices for implementing supply chain security, assessments and plans
 - Requirements and guidance
- ISO 28002:** 2011 Security management systems for the supply chain
 - Development of resilience in the supply chain

- Requirements with guidance for use

ISO 28003:2007 Security management systems for the supply chain

- Requirements for bodies providing audit and certification of supply chain security management systems

ISO 28004-1:2007 Security management systems for the supply chain

- Guidelines for the implementation of ISO 28000
- Part 1: General principles

ISO 28004-3:2014 Security management systems for the supply chain

- Guidelines for the implementation of ISO 28000
- **Part 3:** Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)

ISO 28004-4:2014 Security management systems for the supply chain

- Guidelines for the implementation of ISO 28000
- Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective

and related authentication systems to detect counterfeiting and illicit trade
ISO/TS 18482* Security management system

- Guidance for use
- Fraud risk assessment guidance

ISO 34001* Security management system

- Fraud countermeasures and controls

ISO 18641* Fraud countermeasures and controls

- Terminology

ISO 19564* Product fraud countermeasures and control

- General principles

ISO 19998* Requirements for the content, security and issuance of excise tax stamps

ISO 20229* Guidelines for establishing interoperability among object identification systems to deter counterfeiting identification and illicit trade

LISTADO 5:

ISO 12931:2012 Performance criteria for authentication solutions used to combat counterfeiting of material goods

ISO 16678:2014 Guidelines for interoperable object identification

La correcta aplicación de estas normas nos proporcionará seguridad y fiabilidad, ayudando al líder de seguridad a garantizar la protección integral de su organización, así como de las partes interesadas y sus socios comerciales.

Eduardo Hernández Ruiz

Presidente del Consejo de Seguridad en Cadena de Suministro en México

2.2 La certificación para el aseguramiento de las cadenas de suministro



“En el futuro, la competencia no se dará de empresa a empresa, sino más bien de cadena de suministros a cadena de suministros.”

Michael E. Porter



ISO 28000 - En la prevención del delito

De acuerdo con los delitos configurados en el Código Penal Colombiano, aquellos relacionados contra el patrimonio, algunos contra el orden económico y social, como el lavado de activos, se han convertido en amenazas a la seguridad, que por problemas de orden social, como el desempleo, el narcotráfico, la violencia armada y los insuficientes esfuerzos del Gobierno, hacen que esto represente un riesgo latente para las organizaciones.

Los diferentes delitos y los delincuentes frente a las medidas de control implementadas por las organizaciones, han ido mutando a nuevas modalidades, que han llevado a que los delincuentes actúen de manera estructurada, dinámica e innovadora y con ello han generado nuevas estrategias para delinquir; esta es la razón por la cual la Norma ISO 28000 permite que las organizaciones revisen permanentemente sus matrices de riesgos, identifiquen nuevas vulnerabilidades y generen controles encaminados a reducir la probabilidad de ocurrencia del riesgo y el impacto que pueda causar, acorde con las necesidades propias de cada organización y que mitigan el impacto del actuar delincriminal y a su vez genera la necesidad de evaluar permanentemente la eficacia de los controles implementados, lo que hace que sea un sistema dinámico, en algunos casos redundante, con menor probabilidad de vulneración y que reduce costos.

ISO 28000 - Como minimizar el riesgo al delito

La Certificación del Sistema de gestión de seguridad en la cadena de suministro, con base en la norma ISO 28000, es la evidencia de que las organizaciones que pertenecen a la cadena de suministro tienen la capacidad para controlar las amenazas y vulnerabilidades que pueden afectar la seguridad.

Beneficios de la implementación de un Sistema de Gestión de Seguridad en la Cadena de Suministro con ISO 28000

Dentro de los beneficios de la implementación de un Sistema de Gestión de Seguridad en la Cadena de Suministros con ISO 28000, se encuentran:

- Es una norma que facilita la identificación de amenazas y riesgos de las organizaciones que hacen parte de la cadena de suministros.
- Estimula la generación de controles operacionales encaminados en la reducción de la probabilidad de ocurrencia de los riesgos y la mitigación de los impactos,
- Promueve el cumplimiento de la política y los objetivos de seguridad a través de planes y programas de seguridad, previene la ocurrencia de incidentes que afecten la continuidad del negocio que permite tener organizaciones más resilientes.
- Permite mayor interacción con las partes interesadas y establecer los controles necesarios con los mismos para fortalecer los eslabones de la cadena de suministros.
- Genera mayor confianza en la seguridad de instalaciones, personas y mercancías hasta la entrega de un producto a un cliente/usuario final, minimiza costos pérdidas, siniestros, deterioros, fraude, entre otros delitos.

La gestión en la cadena de suministros, permite a través de actividades sistemáticas la continua identificación de vulnerabilidades, amenazas y riesgos, poner a prueba (cuando es aplicable) las medidas de control, lo cual permite evaluar la eficacia de los controles implementados e implementar nuevas medidas de control.

Aspectos claves de la norma ISO 28000:2007 - Programas de seguridad

En la planificación y el control de los sistemas de gestión de seguridad de la cadena de suministro es clave la determinación de la política, objetivos, planes y programas de seguridad.

Respecto a este último es importante resaltar que, los programas de seguridad deben estar enfocados en el cumplimiento de los objetivos y metas definidos, que deben describir las actividades, los recursos necesarios, las responsabilidades y las autoridades para la realización de las actividades, y el tiempo previsto para que estas se lleven a cabo.



Fuente: Imágenes de Google.

A manera de ejemplo se podría considerar como objetivo y meta de seguridad lo siguiente:

OBJETIVO	META
<p>Reducir las pérdidas de producto en el transporte de mercancía</p>	<p>Reducir en 50% la pérdida de mercancías en dos años, de la siguiente manera: En el primer año se debe reducir: 10% de las averías cuando el producto se encuentre en tránsito. 30% de pérdidas por hurto en los traslados de la bodega principal a puerto.</p> <p>En el segundo año se debe reducir 10% las pérdidas por saqueo durante el traslado de mercancías del puerto a la bodega principal Bogotá zona franca.</p>



Un programa o gestión de seguridad de la mercancía, debería incluir:

- Un indicador general que mida la gestión del programa en relación con uno o más objetivos y metas de seguridad. No es conveniente que se establezcan mediciones que tengan como finalidad el cumplimiento de las actividades del programa.
- La periodicidad de seguimiento. La cual no debería realizarse en periodos definidos, los cuales no deberían ser tan amplios que no permita identificar las desviaciones y la materialización de riesgos y tomar decisiones oportunas, o tan cortos que no permitan evaluar su eficacia.
- Las actividades claves que contribuyen en la intervención del riesgo y que aportan al cumplimiento de los objetivos y de las metas definidas.
- Establecer el tiempo requerido para el cumplimiento de cada una de las actividades (este tiempo debería establecerse en relación con el cumplimiento del objetivo de seguridad).
- Incluir la responsabilidad y autoridad requerida para la eficaz implementación del programa y preferiblemente de cada actividad.
- Los recursos que se requieren para el cumplimiento de las actividades del programa.
- Y definir el resultado esperado de cada actividad, podría contribuir en tener resultados eficaces.

2.3 Buenas prácticas para la continuidad de los negocios, "Gestiones de la Seguridad"



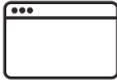
"Los programas o gestiones de seguridad consolidan el valor de la interacción que tienen los actores de la cadena de suministro."



En la presente sección de la guía, se recopilan las "buenas prácticas", que permiten prevenir y controlar "eventos" que afectan la operación y el buen nombre de una organización.

La hemos llamado "gestión de la seguridad", debido a que la actividad de "seguridad" debe ser parte integral de los procesos de la organización, y como tal, se debe administrar e involucrar a todas las personas que integran la empresa.

La presentación de las buenas prácticas en la gestión de seguridad, se realiza en un cuadro, que lleva la siguiente información:

	<p><i>Gestión de la seguridad</i></p>	<p>Título de la buena práctica de la gestión de la seguridad, la cual describe la actividad para gestionar</p>
	<p><i>Propósito</i></p>	<p>Describe el resultado que se obtiene una vez las buenas prácticas sean adaptadas por la empresa.</p>
	<p><i>Eventos para gestionar</i></p>	<p>Indica los potenciales delitos, eventos con impacto negativo, los cuales son gestionados por estas buenas prácticas.</p>
	<p><i>Documentos para la gestión</i></p>	<p>Relaciona los procedimientos, formatos, entre otros documentos, que ayudan a la organización a describir y determinar el método para hacer cumplir las medidas de control.</p>

	<i>Actividades de control para la prevención</i>	Están relacionados los controles que permiten reducir la ocurrencia de un potencial evento con impacto negativo.
	<i>Actividades de control para la detección</i>	Ayudan a identificar la ocurrencia de un potencial evento con impacto negativo.
	<i>Herramientas de control</i>	Describe sitios o páginas Web para realizar consultar y/o tener acceso a información adicional.

A continuación se proponen buenas prácticas o gestiones de seguridad para:

1. El personal propio y subcontratado
2. La capacitación y entrenamiento
3. La selección de los asociados de negocio (clientes, proveedores y terceros)
4. Los datos y la información
5. El control de documentos
6. La infraestructura
7. Otros activos
8. La exportación
9. La importación
10. El transporte de mercancías
11. El producto y/o prestación del servicio
12. Los requisitos legales



1 GESTIÓN DE LA SEGURIDAD PARA EL PERSONAL PROPIO Y SUBCONTRATADO

Propósito



Vincular y mantener personal que le sea confiable para la organización

Eventos para gestionar



- Falsedad personal
- Concierto para delinquir.

Documentos para la gestión



- Procedimiento de selección, control y desvinculación de personal
- Manual de funciones y responsabilidades
- Registro de la visita domiciliaria
- Registro de la verificación de referencias laborales y personales

Actividades de control para la prevención



- Solicitar previamente los documentos requeridos para la contratación de la persona.
- Elaborar un listado con los datos básicos de los colaboradores de la organización.
- Identificar los cargos críticos, dada su responsabilidad y autoridad
- Confirmar la información suministrada por el candidato, antes de la contratación.

Actividades de control para la detección



- Anualmente verificar los antecedentes judiciales
- Cada dos años realizar visita al domicilio del colaborador.
- Anualmente solicitar la actualización de los datos básicos del colaborador
- Realizar prueba de poligrafía de selección, rutina y específicos.

Herramientas de control



- Policía, <http://antecedentes.policia.gov.co:7003/WebJudicial/>
- Expedientes judiciales, <http://procesos.ramajudicial.gov.co/prueba/consultap.aspx>
- Procuraduría, http://www.procuraduria.gov.co/html/servicios/servicios_antecedentes.htm
- Registraduría, <http://web.registraduria.gov.co/servicios/certificado.htm>
- RUAFA, <http://ruafsvr2.sispro.gov.co>
- FOSYGA, <http://www.fosyga.gov.co>
- INTERPOL, <http://www.interpol.int>
- DEA, <http://www.justice.gov>



2 GESTIÓN DE LA SEGURIDAD PARA LA CAPACITACIÓN Y ENTRENAMIENTO

Propósito



Motivar a los colaboradores de la organización en la participación activa para la seguridad

Eventos para gestionar



- Concierto para delinquir
- Cohecho por dar u ofrecer
- Abuso de confianza
- Soborno

Documentos para la gestión



- Programa de capacitación y entrenamiento
- Programa de prevención para no consumo de alcohol y sustancias psicoactivas
- Código de ética
- Procedimiento para el reporte de operaciones sospechosas y señales de alerta

Actividades de control para la prevención



- Incluir dentro de la inducción, las políticas y/o normas de seguridad de la organización
- Realizar actividades de reintroducción, periódicas, para recordar las políticas y/o normas de seguridad
- Análisis de casos presentados, con el fin de identificar oportunidades de mejora

Actividades de control para la detección



- Incluir dentro de la evaluación del desempeño, aspectos relacionados con el cumplimiento de las políticas y/o normas de seguridad
- Realizar inspecciones y/o auditorías a las actividades más sensibles

Herramientas de control



Transparencia por Colombia, <http://transparenciacolombia.org.co/>



3

GESTIÓN DE LA SEGURIDAD PARA ASOCIADOS DE NEGOCIO (clientes, proveedores y terceros)

Propósito



Desarrollar vínculos comerciales con asociados de negocio seguros y confiables

Eventos para gestionar



- Lavado de activos
- Contrabando
- Financiación del Terrorismo

Documentos para la gestión



- Procedimiento de selección y control de asociados de negocio
- Formato de identificación de asociados de negocio (hoja de vida)
- Registro de la visita a instalaciones de los asociados de negocio
- Acuerdo de seguridad para los asociados de negocio
- Manual SIPLAFT / SARLAFT

Actividades de control para la prevención



- Definir el perfil de riesgo de los asociados de negocio, con la descripción de la criticidad en la cadena de suministros
- Solicitar previamente los documentos legales y comerciales que permita conocer al asociado de negocio
- Elaborar un listado de los asociados de negocio seleccionados y autorizados por la organización

Actividades de control para la detección



- Verificar la información del asociado de negocio previamente a la relación comercial y cada año
- Actualizar anualmente la información legal y comercial
- Revisar anualmente los acuerdos de seguridad y actualizarlos cuando sea el caso.
- Realizar visita a las instalaciones del asociado antes de la relación comercial y actualizarla cada dos años.

Herramientas de control



- Lista OFAC, <https://sanctionssearch.ofac.treas.gov/>
- RUES, http://www.rues.org.co/RUES_Web/Consultas
- Supersociedades, <http://www.supersociedades.gov.co/Paginas/default.aspx>



4 GESTIÓN DE LA SEGURIDAD PARA LOS DATOS Y LA INFORMACIÓN

Propósito



Mantener la confidencialidad, integridad y disponibilidad de la información de la organización

Eventos para gestionar



- Acceso abusivo a un sistema informático
- Daño Informático
- Hurto por medios informáticos y semejantes
- Interceptación de datos informáticos
- Suplantación de sitios web para capturar datos personales
- Uso de software malicioso

Documentos para la gestión



- Procedimiento de elaboración de copias de seguridad
- Procedimiento para la creación, modificación y eliminación de usuarios.
- Registro con el inventario de los equipos que manejan y archiva información: computadores y dispositivos móviles.

Actividades de control para la prevención



- Clasificar la información de la organización
- Elaborar un inventario detallado de las computadoras de la organización
- Elaborar un inventario de las aplicaciones que utiliza la organización
- Programa de mantenimiento preventivo de las computadoras
- Asignación de usuarios y contraseñas individuales, y cambio periódico
- Realizar copias de seguridad periódicas y verificar el contenido
- Utilizar programas o software con licencia, o en su defecto de acceso libre.

Actividades de control para la detección



- Utilizar software, antivirus - anti spy
- Implementar firewall, contrafuegos
- Encriptar la información
- Inspecciones a los equipos

Herramientas de control



- Centro Cibernético Policial, <http://www.ccp.gov.co/>
- Homeland Security, <https://www.dhs.gov/topic/cybersecurity>



5

GESTIÓN DE LA SEGURIDAD PARA EL CONTROL DE DOCUMENTOS

Propósito



Mantener la disposición e integridad de los documentos

Eventos para gestionar



- Falsedad material en documento público
- Uso de documento falso
- Violación de datos personales
- Violación de reserva industrial o comercial

Documentos para la gestión



- Procedimiento para la administración del archivo; ingreso, préstamo y retiro de documentos
- Registro con la relación de las firmas de las personas, cargo y el documento autorizado
- Registro con la relación de los sellos de tinta y/o secos utilizados en cada uno de los procesos
- Procedimiento para el control de ingreso y salida de la correspondencia

Actividades de control para la prevención



- Identificar los documentos que utiliza la organización con el título y la fecha de elaboración
- Determinar lugares para que los documentos sean consultados por los trabajadores
- Disponer al interior de la organización, lugares para que los documentos sean ubicados y permitan fácil acceso y consulta.
- Definir puntos al interior de la organización para el almacenamiento de información considerada como confidencial.
- En caso de utilizar documentos reciclados, verificar la información ubicada al dorso de hoja; puede contener información sensible.
- Utilizar picadora de papel, para la destrucción de documentos.
- Mantener los puestos de trabajo ordenados, "escritorios limpios".

Actividades de control para la detección



- Auditorías internas a los documentos

Herramientas de control



- Archivo General de la Nación, <http://www.archivogeneral.gov.co/leyes>



6 GESTIÓN DE LA SEGURIDAD PARA LA INFRAESTRUCTURA

Propósito



Preservar la integridad y funcionamiento de la infraestructura de la organización

Eventos para gestionar



- Sabotaje
- Hurto
- Daño en bien ajeno

Documentos para la gestión



- Registro de las inspecciones a las instalaciones
- Plano de las instalaciones para identificar las áreas consideradas como sensibles y/o restringidas
- Procedimiento para el control de los puntos de ingreso de trabajadores y vehículos

Actividades de control para la prevención



- Identificar y señalar las áreas consideradas como sensibles y/o restringidas
- Elaborar un programa de mantenimiento preventivo
- Capacitar y sensibilizar a los trabajadores en el uso adecuado de los elementos, equipos y herramientas de trabajo
- Controlar las áreas y zonas de lockers
- Usar elementos de control, como candados, que retrinjan (no permitan) el acceso no autorizado.
- Identificar a los trabajadores y visitantes (carnets)
- Contar con el apoyo de los servicios de empresas de vigilancia y seguridad privada legalmente constituidas
- Registrar y controlar los elementos, equipos y/o herramientas que ingresen a las instalaciones

Actividades de control para la detección



- Realizar inspecciones y recorrido a las instalaciones de la empresa
- Programar y ejecutar simulacros o pruebas de vulnerabilidad para comprobar el funcionamiento de las medidas de control
- Contar con dispositivos electrónicos, sistema de circuito cerrado de televisión, CCTV y alarmas

Herramientas de control



- Supervigilancia, <http://www.supervigilancia.gov.co/>



7 GESTIÓN DE LA SEGURIDAD PARA OTROS ACTIVOS

Propósito



Conservar y custodiar los activos de la organización

Eventos para gestionar



- Sabotaje
- Hurto

Documentos para la gestión



- Procedimiento para la adquisición de activos
- Procedimiento para el ingreso y registro de activos
- Programa de mantenimiento preventivo y correctivo de activos
- Políticas y/o normas para la administración del dinero

Actividades de control para la prevención



- Disponer de un listado actualizado de los activos de la organización
- Identificar y/o marcar el número del inventario del activo fijo.
- Acoger los controles sugeridos por las entidades financieras para el control del dinero

Actividades de control para la detección



- Realizar inspecciones periódicas y aleatorias
- Anualmente realizar inventario del 100% de los activos de la empresa

Herramientas de control



- Disponer de un software que permita la administración de los activos de la empresa

8

GESTIÓN DE LA
SEGURIDAD PARA
LA EXPORTACIÓN

Propósito



Asegurar la integridad y la seguridad de los productos con destino a la exportación.

Eventos para gestionar



- Exportación ficticia
- Tráfico de sustancias ilícitas
- Hurto

Documentos para la gestión



- Procedimiento para el empaque y alistamiento del producto de exportación
- Procedimiento para el cargue y despacho del producto de exportación
- Registro de inspección de contenedores
- Registro de inventario de sellos de seguridad
- Registro de las personas que participaron en la operación de cargue y despacho

Actividades de control para la prevención



- Asignar solo al personal autorizado a realizar las actividades de empaque, cargue y despacho
- Instalar sellos de seguridad al contenedor y/o vehículo
- Disponer de los documentos del despacho y compararlos con los productos cargados
- Realizar el transporte del producto con destino a la exportación con empresas confiables; recomendación que sean BASC
- Identificar la carga de exportación
- Utilizar materiales de empaque y/o embalaje diferentes a los utilizados para el mercado local
- Instalar sellos de alta seguridad a las unidades de cargue (vehículo y/o contenedor)

Actividades de control para la detección



- Inspeccionar el contenedor y/o el vehículo previo al cargue
- Utilizar canino para la detección de potenciales sustancias ilícitas
- Realizar inspecciones a los materiales de empaque y/o embalajes utilizados en la exportación

Herramientas de control



- Filmar el proceso de empaque, cargue y despacho a través del Sistema de CCTV
- Tomar registro fotográfico de las mercancías que se van a exportar, así como el vehículo y/o contenedor.



9

GESTIÓN DE LA SEGURIDAD PARA LA IMPORTACIÓN

Propósito



Asegurar la integridad y la seguridad de los productos importados

Eventos para gestionar



- Tráfico de armas
- Hurto
- Lavado de activos
- Contrabando
- Importación ficticia
- Porte de armas de fuego

Documentos para la gestión



- Procedimiento para el descargue, ingreso y ubicación de los productos importados
- Formatos para registrar la información relacionada con el ingreso de los productos

Actividades de control para la prevención



- Verificar los datos de la unidad de carga (vehículo y/o contenedor) previamente al descargue de los productos
- Verificar y registrar el estado del sello de seguridad, precintos y/o candados
- Asignar un responsable de la verificación de los productos recibidos (estado y cantidad)

Actividades de control para la detección



- Utilizar una lista de empaque y/o listado de los productos recibidos para identificar cualquier novedad

Herramientas de control



- Filmar el proceso de recepción de los productos importados
- Tomar registro fotográfico de los productos
- Utilizar software para llevar el control de inventario de los productos.



10

GESTIÓN DE LA SEGURIDAD EN EL TRANSPORTE

Propósito



Mantener la seguridad e integridad de los productos transportados en vehículos.

Eventos para gestionar



- Hurto en la cadena de suministro
- Hurto de automotores
- Tráfico de sustancias para el procesamiento de narcóticos

Documentos para la gestión



- Procedimiento para la elaboración de documentos de transporte
- Procedimiento para el despacho de un vehículo
- Procedimiento para la selección de conductores terceros
- Procedimiento para el seguimiento y monitoreo de un vehículo

Actividades de control para la prevención



- Elaborar un control de las personas responsables de realizar la operación de despacho
- Disponer de un control de firmas y sellos de tinta para autorizar los procesos y documentos de la operación
- Verificar previamente la información del vehículo, conductor y propietario
- Realizar las consultas de los datos del vehículo, conductor y propietario, previamente al despacho

Actividades de control para la detección



- Realizar seguimiento constante al GPS y/o puestos de control
- Disponer de elementos de comunicación para reportar cualquier novedad oportunamente

Herramientas de control



- INVIAS, evasión de peajes, <http://cumbia.invias.gov.co>
- SIMIT, <https://consulta.simit.org.co>
- Placa del vehículo; <http://www.runt.com.co>
- Vehículos de carga, <http://www.runt.com.co>
- Vehículos habilitador transporte internacional, <http://web.mintransporte.gov.co/consultas>
- Licencia de tránsito, <http://web.mintransporte.gov.co>
- Manifiesto de carga, <http://web.mintransporte.gov.co>

 <h1>11</h1> <p>GESTIÓN DE LA SEGURIDAD DEL PRODUCTO Y/O PRESTACIÓN DEL SERVICIO</p>	<p>Propósito </p> <p>Prestar un servicio confiable e íntegro a los clientes</p>	<p>Eventos para gestionar </p> <ul style="list-style-type: none"> • Falsedad marcaria • Estafa • Ofrecimiento engañoso de productos y servicios • Uso ilegítimo de patentes • Usurpación de marcas y patentes
<p>Documentos para la gestión </p> <ul style="list-style-type: none"> • Procedimiento para la prestación del servicio, indicando cada uno de los servicios que ofrece la organización 	<p>Actividades de control para la prevención </p> <ul style="list-style-type: none"> • Verificar la confiabilidad del potencial cliente, antes de enviar la propuesta o cotización del servicio • Elaborar la propuesta, describiendo detalladamente la promesa de valor hacia el cliente • Confirmar la prestación del servicio a través de una solicitud • Suscribir un contrato para formalizar la relación comercial • Utilizar acuerdos de seguridad para determinar los controles de seguridad que ambas partes deben aplicar para la administración de riesgos 	<p>Actividades de control para la detección </p> <ul style="list-style-type: none"> • Elaborar un listado con las señales de alerta, que permitan identificar potenciales actividades ilícitas
<p>Herramientas de control </p>		
<ul style="list-style-type: none"> • Contar con una herramienta (física o magnética) que permita conocer la trazabilidad en la prestación del servicio 		

 <h1>12</h1> <p>GESTIÓN DE LA SEGURIDAD PARA LOS REQUISITOS LEGALES</p>	<p>Propósito </p> <p>Garantizar el cumplimiento de los requisitos legales aplicables a la organización</p>	<p>Eventos para gestionar </p> <ul style="list-style-type: none"> • Omisión de control • Operaciones no autorizadas con accionistas o asociados
<p>Documentos para la gestión </p> <ul style="list-style-type: none"> • Procedimiento para la identificación, implementación y cumplimiento de los requisitos legales 	<p>Actividades de control para la prevención </p> <ul style="list-style-type: none"> • Elaborar un listado con las fuentes de información en donde la organización puede consultar actuales y nuevos requisitos legales 	<p>Actividades de control para la detección </p> <ul style="list-style-type: none"> • Realizar seguimientos periódicos para verificar el cumplimiento de los requisitos legales
<p>Herramientas de control </p>		
<ul style="list-style-type: none"> • Identificar fuentes, http://www.legiscomex.com/ 		

2.4 Diez ideas para controlar los riesgos sociales y criminales en un escenario de posacuerdo



"Las ideas son propuestas, pero en un universo de entornos y posibilidades, la mejor decisión es la alineada con la seguridad."



De cara al rol protagónico de las empresas en Colombia para lograr el propósito de alcanzar la paz, y teniendo en cuenta los retos y desafíos que impone el posacuerdo, a continuación se presentan algunas formas, buenas prácticas y/o recomendaciones que podría desarrollar el sector privado para gestionar de manera adecuada los riesgos emergentes como consecuencia del posacuerdo:

1. Es importante identificar y priorizar impactos y oportunidades, así como retos sociales para tener negocios rentables y seguros.
2. Adoptar herramientas de autodiagnóstico para evaluar la gestión del riesgo criminal y en consecuencia generar oportunidades de mejora, planes de acción, programas o gestiones de seguridad.
3. Vincularse y participar en los programas de agremiaciones y autoridades que tienen como propósito apoyar a las organizaciones que estén interesadas en crear o fortalecer proyectos de encadenamientos, lo que permitirá asumir retos y ser ejemplo de buenas prácticas y casos de éxito. El propósito es que las empresas alineen los riesgos sociales con la seguridad del negocio.
4. Repensar y actualizar con capacidad de adaptación los mapas de riesgos de las empresas, los cuales deben tener un alcance de acuerdo a interés, objeto, cobertura y portafolio del negocio. Para esto es imperante establecer procesos y procedimientos focalizados con indicadores tangibles e intangibles, orientados a fortalecer la prevención criminal, la prevención penal y la reacción eficiente a través de nuevos planes de continuidad del negocio.

5. Reestructurar las políticas de seguridad de acuerdo con la disminución de amenazas a la seguridad nacional, resultantes del actuar de los grupos armados ilegales, a la mutación de las diferentes modalidades delictivas y del crimen organizado en los contextos urbanos y rurales.
6. Fortalecer la relación e interacción con autoridades y vinculación a estrategias para mantener sistemas seguros y controlados de seguridad, haciendo parte de mecanismos de prevención criminal como el FSE de la DIJIN.
7. Actualizar los programas y planes de capacitación. Para esto es importante considerar temas actuales y de coyuntura, con el fin de fortalecer la pedagogía en temas como los acuerdos de La Habana, los roles sociales y empresariales frente a la responsabilidad colectiva de construir seguridad y paz, el nuevo Código Nacional de Policía (Ley 1801 del 29 de julio de 2016), el cual está diseñado para la convivencia y seguridad, la transformación del crimen, las nuevas dinámicas, tendencias sociales, tecnológicas y normativa para el cumplimiento de requisitos legales transversales y del negocio específico, entre otros.
8. Involucrarse y desarrollar compromisos de corresponsabilidad con la seguridad, convivencia ciudadana y la paz, que impacten el desarrollo normal de sus procesos, la seguridad de sus instalaciones, ejecutivos, empleados, activos, información, operación y asociados de negocio.
9. Conocer los planteamientos de diferentes actores del posconflicto, como el Gobierno Nacional, la academia, la empresa, los gremios y asociaciones, así como experiencias y referentes internacionales, con el fin de desarrollar en los líderes de las empresas la capacidad de transformación y adaptación para la normalización del país.
10. Realizar diagnósticos y estudios prospectivos que permitan a la empresa conocer las tendencias criminales y establecer controles efectivos, para lo cual debería considerarse el conocimiento mínimo de modalidades y recomendaciones de prevención. Observe el siguiente ejemplo:

Modalidades del cibercrimen



- > **Defacement:** Es la modificación de páginas Web sin la autorización del administrador del sistema.
- > **Malware:** Programa informático que ejecuta acciones ilegítimas y desautorizadas en un sistema informático.
- > **Ransomware:** Programa informático empleado por los delincuentes para cifrar la información contenida en un computador y luego pedir recompensa.
- > **Spoofing:** Consiste en la suplantación de datos personales para el envío o recepción de información tales como un correo electrónico o dirección IP.
- > **Phishing:** Es la suplantación de sitios Web para capturar datos personales de la víctima.
- > **Usurpación de identidad:** Es el empleo de la información personal de un tercero para obtener de manera ilegítima recursos o beneficios propios de la víctima.
- > **Ingeniería social:** Es la práctica social de obtener información a través del engaño.
- > **Skimming:** Conducta que consiste en la clonación de tarjetas débito y crédito.
- > **Vishing:** Consiste en la ingeniería social llevada a cabo mediante llamadas telefónicas.
- > **Carta nigeriana:** El delincuente ofrece mediante correos electrónicos, herencias, premios o dádivas a cambio de favores.
- > **Smishing:** Es el envío de mensajes de texto que anuncian a la víctima haber ganado supuestos premios y para reclamar debe realizar recargas o consignaciones.

Recomendaciones para la prevención del cibercrimen

- | | |
|--|---|
|  <p>PONER EN PRÁCTICA LA EDUCACIÓN Y LA SENSIBILIZACIÓN DE LOS USUARIOS</p> |  <p>HACER CUMPLIR LAS REGLAS DE NAVEGACIÓN SEGURAS</p> |
| <p>MANTENER LOS SISTEMAS AL DÍA</p>  | <p>UTILIZAR CONTRASEÑAS SEGURAS Y MANTENERLAS SEGURAS</p>  |
|  <p>TENER CUIDADO AL DESCARGAR ARCHIVOS ADJUNTOS EN CORREOS E.</p> |  <p>REALIZAR Y REVISAR COPIAS DE SEGURIDAD DE LOS DATOS DE NEGOCIO E INFORMACIÓN</p> |
| <p>APLICAR SEGURIDAD DE DISPOSITIVOS MÓVILES</p>  | <p>NO BRINDAR INFORMACIÓN FINANCIERA A TRAVÉS DE LLAMADAS TELEFÓNICAS</p>  |
|  <p>NO INGRESAR A LA BANCA VIRTUAL A TRAVÉS DE LINK EN CORREOS</p> |  <p>INFORMAR AL CAIVIRTUAL PARA RESOLVER INQUIETUDES</p> |

Mayor Gelga Buitrago Martínez

Jefe Área Asistencia y Cooperación para la Policía Judicial, Frentes de Seguridad Empresarial

3

CAPÍTULO



Capacidades
de respuesta
Institucional

3. CAPACIDADES DE RESPUESTA INSTITUCIONAL - CAJA DE HERRAMIENTAS

3.1 Conceptualización de la prevención y su desarrollo en la Policía Nacional



“La prevención, implica contrarrestar los factores de riesgo y las amenazas que las generan.”



Los desafíos de un país que acoge la idea de construir paz, convivencia y seguridad, implican transformaciones sociales, políticas, culturales y por supuesto institucionales. La Policía Nacional de Colombia, como una de las instituciones llamadas a la consolidación de estos procesos de cambio, realiza constantemente un ejercicio introspectivo de pensarse como un actor propositivo, constructor y participante en dinámicas de tejido social, desarrollo económico y garante de derechos, lo que supera los paradigmas tradicionales de los cuerpos de policía.

Bajo esta premisa, además de fortalecer todo el desarrollo operativo, basado en la inteligencia policial y la investigación criminal, se arraiga en lo más cotidiano del servicio de policía, el trabajo con las comunidades e instituciones públicas y privadas, de tal manera, que se involucren en la solución de las problemáticas delictuales y sociales, que se fundamentan en aspectos estructurales y culturales.

Teniendo en cuenta lo anterior y en el marco del “Plan Nacional de Desarrollo 2014-2018, Todos por un nuevo país”, la “Política de Defensa y Seguridad para la Nueva Colombia 2015-2018”, y el “Plan Estratégico Institucional 2015-2018, Comunidades Seguras y en Paz”, ha concentrado sus esfuerzos en la consolidación de una política institucional hacia la prevención de violencias, delitos y conductas contrarias a la convivencia, y a la persecución del actor criminal, que tiene por intención la articulación de las capacidades institucionales y de la institucionalidad, a fin de contribuir en el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, desde las expectativas de actores públicos, privados y sociales en los contextos locales y nacionales.

Considerando la trascendencia de la constitución política de 1991, cabe señalar el proceso evolutivo del servicio de policía que la ha

llevado a convertirse en un referente internacional, a partir de la premisa de concentrar los esfuerzos hacia la prevención de violencias, delitos y conductas contrarias a la convivencia y la persecución del actor criminal. En ese orden de ideas, se reseña conceptualmente estos, en el marco de los intereses de actores públicos, privados y sociales.

Prevención de violencias, delitos y conductas contrarias a la convivencia

Desarrollo metodológico que implica identificar, comprender, caracterizar, priorizar, los riesgos, causas y factores que inciden en la ocurrencia de fenómenos sociales y delictuales en los territorios, los cuales tienen efecto en las dinámicas económicas, políticas y culturales; es decir, comprensión contextual y diferencial, la cual plantea un panorama detallado a fin de intervenirlos con la articulación de las capacidades institucionales y de manera corresponsable entre los diversos actores, públicos, privados y sociales.

Así las cosas, de acuerdo con la doctrina generada por el Área de Prevención de la Dirección de Seguridad Ciudadana de la Policía Nacional, como dueña del proceso, es el conjunto de estrategias articuladas y sistemáticas, orientadas a disminuir la probabilidad de ocurrencia de las violencias, delitos y contravenciones en contextos específicos.

La prevención, implica **contrarrestar** los **factores de riesgo** y las **amenazas** que las generan, haciendo necesario potenciar los factores protectores de manera corresponsable.

El Centro de Estudios en Seguridad Ciudadana, CESC, de la Universidad de Chile, que contribuye en el diseño de políticas públicas en materia de seguridad ciudadana, define los tipos de prevención, así:

a) Tipos de prevención

Prevención Primaria: dirigida a la población en general y, comúnmente, responde a necesidades específicas, actuando sobre los contextos sociales y situacionales que favorecen la violencia.

Prevención Secundaria: dirigida a grupos de riesgo específicos y sus necesidades (niños, jóvenes o mujeres), que ya han tenido algún problema producto de la violencia (entornos) y que requieren tratamiento, intervención y apoyo para evitar la revictimización, o bien para que no se conviertan en futuros victimizadores.

Prevención Terciaria: va dirigida a grupos específicos de personas que han cometido infracciones a la ley, que han ingresado al sistema penal, buscando promover su rehabilitación, restitución y reparación y que pueden reincidir en fenómenos relacionados con violencias, delitos y conductas contrarias a la convivencia.

b) Niveles de atención en prevención de violencias, delitos y conductas contrarias a la convivencia

Prevención social: actúa sobre factores de riesgo personales o psicológicos y sociales, estos últimos muchas veces de carácter estructural como son la pobreza y marginalidad. Estas iniciativas pueden estar dirigidas a grupos de alto riesgo social y van desde el ámbito familiar (prevención temprana de la violencia intrafamiliar) hasta la educación (mediación de conflictos en la escuela) o la salud (programas de nutrición infantil). La prevención social puede ser un poco específica en su dimensión de seguridad, debido a que la seguridad sería un efecto a largo plazo del esfuerzo concertado de diversas políticas públicas.

Prevención situacional: actúa sobre factores de proximidad o ambientales en estrecha relación con las situaciones provocadoras de violencia y la actividad delictual. Ellos cubren el ámbito urbano y rural (recuperación de espacios públicos, mejor iluminación, vías de acceso, infraestructura). La prevención situacional opera anticipándose al razonamiento del actor criminal, interviniendo los factores que le facilitan su actuar. Sin embargo, el accionar del actor criminal es siempre dinámico, buscando las formas de sortear los obstáculos, por lo que las medidas situacionales deben estar en constante transformación.

Prevención comunitaria: combina elementos de ambos ámbitos, el social y el situacional, y su característica más definitoria ha sido la participación ciudadana, especialmente definida en lo local. Lo que significa la inclusión de las comunidades en la solución de las problemáticas identificadas, así como el involucramiento en proyectos de corto alcance enfocados a la prevención social o situacional.

De igual manera, durante este proceso evolutivo, respecto a la prevención de violencias, delitos y conductas contrarias a la convivencia, cobra fuerza el concepto de Riesgo social, definido así:

c) Riesgos sociales

Acudiendo al concepto del profesor Edgar Mendoza, el riesgo social “Conlleva a situaciones y escenarios de riesgo, pero se debe tener en cuenta que están dentro de un contexto histórico, económico, político y social en determinada época o período” (...) “son parte de las sociedades donde se encuentran diversos grupos sociales que poseen un patrimonio cultural, memoria histórica, identidades, tradiciones culturales, prácticas de socialización, imaginarios sociales, leyendas, mitos, patrimonios arqueológicos, danzas, canciones, costumbres, creencias, rituales, etc., que existe la posibilidad de que puedan estar amenazadas y en peligro de desaparición por diversos motivos como desastres nucleares, industria de minerales o el proceso de homogenización de la globalización cultural”.

El riesgo social en la comprensión de la Policía Nacional corresponde a los peligros a los que se enfrentan los grupos sociales o comunidades en un territorio, que amenazan sus hábitos, costumbres, símbolos y prácticas culturales, los cuales se encuentran enmarcados en dinámicas económicas, políticas y sociales.

En este orden de ideas, las amenazas están relacionadas con la violencia, concepto que se encuentra incorporado en la doctrina de la Policía Nacional, y que se ha referenciado del sociólogo Johan Galtung, para evidenciar la relación entre los riesgos sociales y los factores que inciden en ellos; es así que la violencia cultural hace relación a “aquellos aspectos de la cultura, el ámbito simbólico de nuestra existencia y cotidianidad (materializado en religión e ideología, lengua y arte, ciencias empíricas y ciencias formales), que puede utilizarse para justificar o legitimar violencia directa (homicidios, lesiones, violaciones, hurtos, entre otros) y la violencia estructural (ausencia de mínimos vitales, educación, salud, inclusión).

Factores estructurales: corresponde a esos componentes del orden estructural que afectan los mínimos vitales, los cuales están relacionados con las necesidades básicas insatisfechas de una población, y que plantea un riesgo o amenaza a las construcciones sociales, económicas, políticas y culturales.

Factores Socioculturales: corresponde a los componentes del orden cultural que afectan la convivencia y seguridad ciudadana y se fundamenta en las relaciones de aceptación, respeto, solidaridad, inclusión que se han construido colectivamente.

A partir del anterior contexto y como parte del desarrollo mencionado, se diseña y crea el Sistema de Prevención, Convivencia y Seguridad Ciudadana, el cual tiene por intención armonizar las capacidades de respuesta operacional con que cuenta la policía Nacional, a fin de contrarrestar los fenómenos sociales y de violencia, que afectan la convivencia y seguridad ciudadana. Aquí su descripción.

Sistema de Prevención, Convivencia y Seguridad Ciudadana, SPCSC

El Sistema de Prevención, Convivencia y Seguridad Ciudadana, SPCSC, es un sistema abierto, jerarquizado, constituido por cuatro subsistemas: estructura, doctrina, capacidades y servicio de policía; los cuales interaccionan entre sí (circularmente) según unas reglas de comportamiento y unas funciones dinámicas institucionales que están en constante intercambio y, que tiene como finalidad contribuir en el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz.



El desafío del Sistema de Prevención, Convivencia y Seguridad Ciudadana, SPCSC, se concentra en la articulación y dinamización que debe darse en la vivencia relacional que continuamente se presenta en los entornos y escenarios de perturbación a la seguridad, no solo del Estado y su institucionalidad, sino también en las necesidades de la población en los contextos locales.

El Sistema de Prevención, Convivencia y Seguridad Ciudadana reconoce la importancia del Modelo Nacional de Vigilancia Comunitaria por Cuadrantes, desde el ejercicio corresponsable desplegado como uno de sus principios, en el marco de la generación de un servicio de policía que contemple en el cuadrante el fortalecimiento, la coordinación, el trabajo en equipo, la promoción de cultura ciudadana y las relaciones

de confianza con los ciudadanos enfocados a la solución de problemas desde su territorio.

Este sistema se construye como una acción relacional con el Estado, es decir, su diagnóstico, formulación y desarrollo implica la participación y articulación de diversos actores públicos, privados y del tercer sector (Sociedad civil); la Policía Nacional es un actor en estas dinámicas, que contribuye en la identificación de las problemáticas y en adelantar actividades de prevención y participación ciudadana para afrontarlas.

Programas de prevención institucionales

Redes

- Red Empresarial Frente de Seguridad Empresarial
- Ciudadanos en Red
- Red de Apoyo y Comunicaciones
- Red de Apoyo y Solidaridad Ciudadana

Cultura Ciudadana

- **Cívica:** Infantil, Juvenil y de Mayores
- **Campañas institucionales de sensibilización:**

- Yo no pago, yo denuncio
- Prevención vial: transporte, usuarios (conductores, pasajeros, peatones)
- Infancia y adolescencia
- Estrategia psicosocial de prevención frente al tráfico de sustancias ilícitas.
- Vínculos con la comunidad - Acciones culturales y lúdicas

Corresponsabilidad

- **Gestión interinstitucional para la educación ciudadana:**

- Jóvenes a lo bien
- Asesoría de proyectos productivos
- Abre tus ojos
- Escuelas de Seguridad Ciudadana
- Estrategia de comportamientos asociados a la siembra de cultivos ilícitos
- Programa escolarizado para la prevención del uso y abuso de las drogas y la violencia

Marco normativo

- 3.1. Ley 62 de 1993, del 6 de agosto, “Por la cual se expiden normas sobre la Policía Nacional, se crea un establecimiento público de seguridad social y bienestar para la Policía Nacional, se crea la Superintendencia de Vigilancia y Seguridad Privada y se reviste de facultades extraordinarias al Presidente de la República”.

Sistema Nacional de Participación Ciudadana: Artículo 25. Sistema Nacional. La Policía Nacional desarrollará un sistema nacional integral de participación ciudadana, institucional y descentralizada, con el objeto de fortalecer las relaciones entre el ciudadano y la institución, estableciendo mecanismos efectivos que permitan, que se expresen y sean atendidos distintos intereses sectoriales y regionales atinentes al servicio de Policía y a la seguridad ciudadana.

- 3.2. Ley 1453 de 2011, del 24 de junio, Ley de seguridad ciudadana. “Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad”.
- 3.3. Ley Estatutaria 1757 del 6 de julio de 2015, “Por la cual se dictan disposiciones en materia de promoción y protección del derecho a la participación democrática”.

Artículo 1. Objeto. El objeto de la presente ley es promover, proteger y garantizar modalidades del derecho a participar en la vida política, administrativa, económica, social y cultural, y así mismo a controlar el poder político.

Intendente Hernán Alfonso Ramírez Rodríguez
Responsable de articulación del servicio en prevención
Dirección de Seguridad Ciudadana

3.2 Red de prevención Criminal para el Posacuerdo



Frente de Seguridad Empresarial FSE - DIJIN

1. Antecedentes

La Policía Nacional a través de la DIJIN, desde el año 2001 en su rol institucional de lucha contra las manifestaciones delictivas que afectan la seguridad y convivencia ciudadana en un espectro integral de la sociedad, puso en marcha el Frente de Seguridad Empresarial como un programa especializado de prevención, para atender las necesidades del sector empresarial, identificándolo como estratégico, para atender el nivel de riesgo del sector productivo del país, conforme a sus operaciones en las que se exponen cuantiosas sumas de dinero, en el diario ejercicio del desarrollo de la actividad empresarial en Colombia.

Fórmula conjunta que no tardó en surtir efectos positivos de mutuo beneficio, cimentados en la optimización de los canales de comunicación masivos, que facilita la tecnología, en un escenario de interacción en tiempo real con la comunidad empresarial, generando sentido de corresponsabilidad en el sector privado, entendiendo de esta manera que su papel resulta preponderante a la hora de controlar y mitigar los riesgos asociados a la seguridad, conscientes del impacto corporativo en aspectos económicos, reputacionales y de confianza de negocios en el ámbito nacional e internacional, de cara a una tendencia comercial cada vez más globalizada.

De la mano con la dinámica institucional y producto de la masiva aceptación del programa de prevención empresarial, hoy su formulación estratégica se proyecta desde un modelo bifocal (público-privado) y multisectorial (amplio sector de cobertura empresarial).

Con el ánimo de acercar más la institución a los sectores y fortalecer el intercambio de información, el programa ofrece en el marco de su portafolio de servicios, entrenamientos mensuales, visitas técnicas en campo, asesorías especializadas, mesas casuísticas, recepción de denuncias, suministro de información estadística de criminalidad, análisis para estudios de asociados de negocio, entre otros. Al igual que el fomento de un encuentro anual, en el que la Policía Nacional, a través de la Dirección de Investigación Criminal e INTERPOL, convoca al nivel gerencial del sector privado para compartir temáticas de su interés, relacionadas con la prevención para concientizar la responsabilidad y compromiso que debe generarse desde el sector privado en los temas de seguridad.

2. Formulación en la estructura institucional

De conformidad con lo dispuesto en la Resolución 05839 DIPON-DIJIN del 31 de diciembre del 2015, "Por la cual se define la estructura orgánica interna de la Dirección de Investigación Criminal e INTERPOL, se determinan las funciones de sus dependencias y se dictan unas disposiciones", es la dependencia del área de asistencia y cooperación para investigación judicial, encargada de coordinar con los diferentes organismos del Estado, entidades públicas y privadas a nivel nacional e internacional, el apoyo necesario en procura de generar y desarrollar estrategias encaminadas a la prevención y control de las modalidades delictivas que afectan a los diferentes sectores productivos, en el marco de la interacción entre los diferentes actores de la cadena de suministro, en los procesos de importación y exportación desde un modelo bifocal (sector público - privado) y multisectorial.

3. Proceso de vinculación

3.1 Presentación carpeta de vinculación

La empresa interesada en adherir voluntariamente a los compromisos de corresponsabilidad inherentes a la vinculación al Frente de Seguridad Empresarial, deberá remitir con destino al funcionario de policía designado como responsable del programa en su jurisdicción, una carpeta con la documentación que a continuación se relaciona e iniciar el proceso que a continuación se describe.

- › Formulario de inscripción en original con todos sus campos diligenciados firmado por el Representante Legal.
- › Carta motivada de consentimiento de consulta para estudio de seguridad, dirigida al Jefe de la Seccional de Investigación Criminal con membrete de la entidad y firma del Representante Legal en original.



- › Dos recomendaciones de empresas que gocen de público reconocimiento, con las que haya realizado vínculos comerciales en original y reciente que le acrediten su trayectoria y seriedad para pertenecer al Frente de Seguridad Empresarial.
- › Listado impreso del personal (solo si son menos de 30), si son más de 30, un listado en medio magnético (CD) en Excel, tres columnas: número, nombres y apellidos completos, números de cédula (sin puntos ni comas). Con oficio adjunto de solicitud de consulta de antecedentes judiciales firmada por el Representante Legal, en el que exprese tácitamente el cumplimiento a lo dispuesto en la Ley Estatutaria 1581 del 2012 y su Decreto reglamentario 1377 de 2013 (Habeas Data, consentimiento expreso del titular).
- › Listado de vehículos al servicio de la empresa, impreso.
- › Certificado de Cámara de Comercio original y reciente.
- › Copia resolución de Superintendencia o Ministerio que regule la actividad de su objeto social (si aplica).

3.2 Visita técnica pre-vinculación

Es el desplazamiento previamente programado y autorizado a las instalaciones físicas de la empresa, por parte del funcionario policial designado como responsable del estudio de vinculación de empresas y el correspondiente Jefe del FESEM, cuyo objeto principal es la validación de la existencia real de la empresa y la verificación de la política de seguridad integral corporativa, mediante una percepción directa; identificando oportunidades de aportes de fortalecimiento en materia de prevención de delitos, mitigación de riesgos, compromiso con la Investigación Criminal y corresponsabilidad en general con la seguridad y la Policía Nacional.



Son los componentes que se deben inspeccionar, los cuales permitirán establecer un diagnóstico general del estado de seguridad empresarial, inspirados por estándares internacionales de seguridad, sistemas de gestión, procesos y campañas institucionales, factores de oportunidad en apoyo a la investigación judicial transversales a la corresponsabilidad con la seguridad corporativa que servirán de insumo para conminar la prevención de delitos y contrarrestar los factores criminales que pueden afectar la continuidad de negocios e impactar el clima de confianza y seguridad de negocios al sector productivo del país, a través de compromisos de adhesión voluntaria asumidos por la empresa, que quedarán plasmados en el acta de reunión.

3.3 Ceremonia de vinculación



Acto institucional al que se convocan al Representante Legal y al Representante ante el FSE de la empresa, el cual ha superado el proceso de estudio de vinculación en la que se socializará ampliamente los beneficios y compromisos de las empresas vinculadas y se oficializará la vinculación a través de la firma del Acta de vinculación.

4. Frentes de cobertura para integrar el Frente de Seguridad Empresarial DIJIN

Se refiere a los sectores empresariales que la Policía Nacional, por considerar de mayor vulnerabilidad frente al accionar criminal, ha identificado como de tratamiento prioritario.

4.1 Sector Privado

- › Organizaciones y empresas que luchan contra la falsificación de marcas, patentes y Derechos de Autor.

Se refiere a las empresas u organizaciones gremiales que producen o fomentan la propiedad intelectual, cuyas producciones, creaciones e invenciones están protegidas y registradas en la Dirección Nacional de Derechos de Autor y (o) Superintendencia de Industria y Comercio.



- › Sector minero energético e hidrocarburos.



Se refiere a las empresas legalmente constituidas y sus respectivas asociaciones gremiales, autorizadas y destinadas a la producción de energía y extracción de minerales e hidrocarburos, con contratos y licencias vigentes por parte de la Agencia Nacional de Hidrocarburos, ANH, y la Agencia Nacional Minera, ANM.

- › Sector Financiero, asegurador y transporte de valores.

Hace referencia a las entidades bancarias legalmente constituidas, vigiladas por la Superintendencia Financiera, empresas transportadoras de valores autorizadas por la Superintendencia de Vigilancia



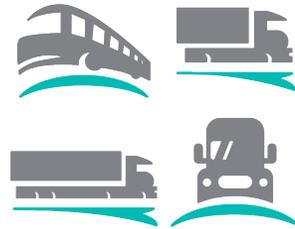
y Seguridad Privada y Firmas Aseguradoras legalmente constituidas y reconocidas en Colombia. Y sus respectivas organizaciones gremiales.

- › Empresas de Vigilancia y Seguridad Privada, servicios autorizados por la Superintendencia de vigilancia y seguridad privada.

Cooperativas de Vigilancia, Empresas Arrendadoras, Empresas Asesoras, Consultoras e Investigadoras, Empresas Blindadoras, Empresas de Vigilancia con Armas, Empresas de Vigilancia sin Armas, Escuelas de Capacitación en Seguridad Privada, Asesores, Consultores e Investigadores.

- › Actores de la cadena de suministro (generadores de carga, bodegas de almacenamiento, almacenes generales de depósito autorizados, agente de carga internacional, transportadores de carga, puertos, aeropuertos, navieras, operadores logísticos, distribución y grandes superficies y actores que interactúan en la importación y exportación de mercancías).

Se refiere a las empresas y organizaciones gremiales que interactúan en el conjunto relacionado con recursos y procesos que comienza con el suministro de materias primas y se extiende hasta la entrega de productos o servicios al usuario final, incluidos los medios de transporte.



- › **Transportador Terrestre Automotor de Carga:**

Persona natural o jurídica, organizada legalmente en Colombia, que en nombre propio o representación de terceros ejerce como actividad principal la prestación de servicios de transporte de carga.

Servicio público de transporte terrestre automotor de carga. Es aquel destinado a satisfacer las necesidades generales de movilización de cosas de un lugar a otro, en vehículos automotores de servicio público a cambio de una remuneración o precio, bajo la responsabilidad de una empresa de transporte legalmente constituida y debidamente habilitada en esta modalidad (Con la debida habilitación por el Ministerio de Transporte).

- › **Generadores de carga:** Empresas destinadas a la actividad Industrial que a través de un conjunto de procesos y actividades que tienen como finalidad transformar las materias primas en productos elaborados o semielaborados, destinados a su comercialización (mercancías). Además de materias primas, para su desarrollo.



- › **Bodegas de almacenamiento:** Empresas destinadas a rentar espacio destinado, bajo ciertas condiciones de almacenamiento de distintos bienes.

› **Almacenes generales de depósito autorizados:** Persona jurídica sometida al control y vigilancia de la Superintendencia Bancaria, a quien la Dirección de Impuestos y Aduanas habilita un lugar para cumplir labores de almacenamiento de mercancías, bajo control aduanero de cualquier usuario del comercio exterior.



› **Agente de carga internacional:** Persona jurídica, cuyo objeto social es la consolidación y desconsolidación de carga internacional, para maximizar el aprovechamiento de rutas y fletes, para lo cual requieren de autorización otorgada por la Dirección de Impuestos y Aduanas Nacionales. Estos usuarios no pueden ser sociedades de intermediación aduanera, ni depósitos públicos o privados.



› **Comercializadora internacional (CI):** Persona jurídica, cuyo objeto social es servir de instrumento de apoyo a las exportaciones, orientando sus actividades hacia la promoción y comercialización de productos colombianos en los mercados externos, para lo cual se requiere contar con la inscripción ante el Ministerio de Comercio, Industria y Turismo o autorización otorgada por la Dirección de Impuestos y Aduanas Nacionales.

› **Depósito público de apoyo logístico internacional:** Persona jurídica a la cual la Dirección de Impuestos y Aduanas Nacionales habilita un lugar en los puertos de servicio público, para el almacenamiento de mercancías bajo control aduanero, de cualquier usuario del comercio exterior. Durante el almacenamiento la mercancía podrá ser sometida a los procesos de conservación, acondicionamiento, manipulación, mejoramiento de la presentación, acopio, empaque, reempaque, clasificación, marcación, preparación para la distribución, reparación o limpieza. No podrá tener adicionalmente la calidad de sociedad de intermediación aduanera, transportadora, agente de carga internacional u operador de transporte multimodal.

› **Depósito privado aeronáutico:** Persona jurídica nacional de transporte aéreo regular de pasajeros y/o carga a la cual la Dirección de Impuestos y Aduanas Nacionales habilita un lugar para el almacenamiento de material aeronáutico que venga consignado a dichas empresas. Debe tener igualmente la calidad de transportador nacional del régimen de importación y exportación, y no podrá tener adicionalmente la calidad de sociedad de intermediación aduanera, agente de carga internacional u operador de transporte multimodal.

› **Depósito público:** Persona jurídica a la cual la Dirección de Impuestos y Aduanas Nacionales le habilita un lugar para almacenar, bajo control aduanero, mercancía de cualquier usuario del comercio exterior. No podrá tener adicionalmente la calidad de sociedad de intermediación aduanera, usuario aduanero permanente, transportador, agente de carga internacional u operador de transporte multimodal.

› **Exportador:** Persona natural o jurídica, que realiza operaciones de exportación de bienes o servicios con destino a otros países o a zona franca industrial de bienes y servicios.



› **Importador:** Persona natural o jurídica que realiza operaciones de importación de bienes o servicios desde otros países o desde zona franca industrial de bienes y servicios.



› **Operador de transporte multimodal:** Persona jurídica inscrita como operador de transporte multimodal ante el Ministerio de Transporte, que cuenta con autorización otorgada por la Dirección de Impuestos y Aduanas Nacionales, para realizar operaciones de transporte multimodal de carga por el territorio aduanero nacional. No puede tener la calidad de sociedad de intermediación aduanera o depósito público o privado.

› **Sociedad de intermediación aduanera:** Persona jurídica autorizada por la Dirección de Impuestos y Aduanas Nacionales, para ejercer la actividad de intermediación aduanera en las operaciones de importación, exportación y tránsito aduanero. No puede tener a su vez la calidad de depósito público o privado, transportador, agente de carga internacional, ni empresa de transporte nacional para el tránsito aduanero.

› **Titular de puertos y muelles de servicio público o privado:** Persona jurídica poseedora de concesión para operar puertos o muelles marítimos o fluviales de servicio público o privado, habilitada por la Dirección de Impuestos y Aduanas Nacionales para el manejo de la operación de entrada y salida de carga del territorio aduanero nacional. No puede tener la calidad de sociedad de intermediación aduanera.

› **Transportador aéreo régimen de importación y/o exportación:** Persona natural o jurídica, organizada legalmente en Colombia, que en nombre propio o representación de terceros ejerce como actividad principal la prestación de servicios de transporte internacional de carga y/o pasajeros. No puede tener la calidad de sociedad de intermediación aduanera.



› **Usuario comercial zona franca:** Persona jurídica autorizada para desarrollar actividades de mercadeo, comercialización, almacenamiento o conservación de bienes, en una o varias zonas francas.

› **Usuario operador de zona franca:** Persona jurídica, autorizada por el Ministerio de Comercio, Industria y Turismo o por la Dirección de Impuestos

y Aduanas Nacionales, para dirigir, administrar, supervisar, promocionar y desarrollar una o varias zonas francas, así como para calificar a sus usuarios.

- **Transportador marítimo régimen de importación y/o exportación:** Persona natural o jurídica, organizada legalmente en Colombia, que en nombre propio o representación de terceros ejerce como actividad principal, la prestación de servicios de transporte internacional de carga. No puede tener la calidad de sociedad de intermediación aduanera.
- **Aeropuerto de servicio público o privado:** Persona jurídica administradora o poseedora de concesión para operar aeropuertos de servicio público o privado, habilitada por la Dirección de Impuestos y Aduanas Nacionales para el manejo de la operación de entrada y salida de carga al o desde el territorio nacional. La habilitación se otorga por Decreto del gobierno nacional o por resolución de carácter particular expedida por la DIAN.
- **Transportador fluvial régimen de importación y/o exportación:** Persona natural o jurídica, organizada legalmente en Colombia, que en nombre propio o representación de terceros ejerce como actividad principal la prestación de servicios de transporte fluvial de carga. No puede tener la calidad de sociedad de intermediación aduanera.

4.2 Sector Público y Gremial

- Programas de Presidencia de la República y Entidades Territoriales.
- Programas Institucionales (Policía Nacional).
- Cámaras de Comercio y Organizaciones gremiales sin ánimo de lucro.
- Superintendencias.
- Programas de Responsabilidad Social Empresarial.
- Agencias de Cooperación Internacional, embajadas y respectivas agregadurías.
- Organizaciones de integración y tratados internacionales suscritos por Colombia.

5 Oferta de servicios Frente de Seguridad Empresarial DIJIN

Relación de beneficios sin costo a los que acceden las empresas vinculadas, en reconocimiento y estímulo a la corresponsabilidad con la seguridad.

- **Entrenamiento en prevención de delitos:** Espacios académicos de capacitación mensual mediante convocatoria masiva, en entrenamiento y sensibilización de la prevención de delitos, dirigida a representantes de las empresa vinculadas, en las que se difundirá la dinámica delictiva (modus



operandi) para plantear medidas de mitigación y buenas prácticas, afianzando básicamente en disciplinas periciales que permitan adquirir fundamentos mínimos para la detección temprana de amenazas y riesgos potenciales de origen delincriminal, que puedan afectar la continuidad de negocios como aporte al fortalecimiento de competencias individuales al talento humano de las empresas vinculadas.

- › **Mesas Técnicas Sectoriales.** Espacios de retroalimentación participativa por sectores similares de negocio, en los que se construya de manera conjunta productos y ayudas que faciliten gestionar los riesgos en seguridad empresarial.



- › **Atención de Consultas:** Previo cumplimiento de consentimiento expreso del titular Ley 1581 de 2012, la empresa podrá acceder a la consulta de antecedentes judiciales vigentes, para uso exclusivamente interno y soporte en la toma de decisiones a través del operador del Frente de Seguridad Empresarial.
- › **Operador exclusivo:** Atención personalizada de operador idóneo en sistemas de gestión en la seguridad empresarial, en ámbitos de acciones preventivas y de reacción ante siniestros con capacidad de articular las capacidades de la Policía Nacional, de conformidad con la especificidad y jurisdicción de la necesidad en seguridad empresarial.
- › **Boletines Diarios de Novedades:** Suministro diario de boletín electrónico en el que se difunden recomendaciones de seguridad, buenas prácticas, resumen de noticias, novedades viales a nivel nacional y convocatorias a eventos liderados por el FSE.
- › **Información Estadística Criminal:** Acceso al suministro de información estadística criminal, conforme a los tipos penales y modalidades delictivas registradas a nivel nacional determinada por extremos de tiempo, descripción geográfica y variables comparativas conforme a las especificaciones del requerimiento.
- › **Asistencia y Asesoría:** Orientación en el proceso penal, entidades intervinientes y participación efectiva en el desarrollo investigativo.



- › **Participación en escenarios de retroalimentación:** Acceso participativo en mesas técnicas, Encuentro Anual Nacional e Internacional del Frente de Seguridad Empresarial y demás espacios que faciliten el fortalecimiento de competencias en el gestionamiento de riesgos y seguridad empresarial.

- › **Encuentro Anual Nacional e Internacional FSE:** Asistencia sin costo al evento anual que convoca al mando institucional, funcionarios de alto gobierno y los Representantes Legales de las empresas con vinculación vigente, en un escenario de alto nivel de contextualización global en el manejo de temas inherentes a la seguridad empresarial.

6 Responsabilidad del empresario

- › Suministrar la información necesaria al FSE para atender sus propios requerimientos y los de la Policía Nacional a través de la DIJIN e INTERPOL.
- › No se puede utilizar el logo, ni las actividades del FSE como un valor agregado para la comercialización de servicios, campañas, propagadas u otro tipo de actividades internas de cada empresa.
- › Participar activamente en las convocatorias, capacitaciones y demás actividades que desarrolle el FSE con sus afiliados en búsqueda de su seguridad; de no ser posible su asistencia enviar un delegado.
- › Contar con procedimiento de selección de personas naturales y jurídicas con las que sostenga vínculos laborales y comerciales en el ámbito de selección y mantenimiento posterior.
- › Brindar la información necesaria y oportuna en lo relacionado con personas que tengan requerimiento vigente por parte de las autoridades; si se tiene conocimiento dar la ubicación de las personas.



7 Medidas sancionatorias

- › El Representante Legal de la empresa vinculada otorga la facultad discrecional de admisión y permanencia en el programa de adhesión voluntaria Frente de Seguridad Empresarial de la DIJIN (libre de costo económico): a la Policía Nacional y/o por baja calificación (menor de 60 puntos) en los 10 criterios de permanencia (activa participación). La desvinculación del programa conllevará la suspensión por término de un año, que una vez transcurrido la empresa podrá volver a postularse para surtir el proceso de vinculación.



- › El FSE podrá suspender el suministro de información a aquellas personas jurídicas, agremiaciones y demás entidades vinculadas que incumplan o dilaten sus compromisos de colaboración con las autoridades o activa participación, o cuyas acciones pongan en peligro el buen nombre o algunas de las normas contenidas en el reglamento de organización y funcionamiento del Frente de Seguridad Empresarial de la Dirección de Investigación Criminal e INTERPOL.

- > La permanencia en el programa FSE en calidad de empresas vinculada lleva inmerso el compromiso de legalidad, compañerismo, solidaridad, respeto y adecuado uso de los canales de comunicación. Al igual que la cultura de legalidad y prevención en sus procedimientos, facilitando la ubicación de las personas con requerimientos vigentes por parte de las autoridades, y cualquier acto contrario habilitará de manera automática la suspensión de servicios o la desvinculación del programa conforme a la gravedad de la infracción.
- > Respetar el buen nombre del FSE y utilizar los canales adecuados de comunicación ante cualquier eventualidad.



8 Criterios de permanencia de las empresas vinculadas al Frente de Seguridad Empresarial DIJIN



Se refiere a los criterios de compromiso que adquiere la empresa en su calidad de vinculada al FSE, su evaluación deberá superar los 60 puntos para su permanencia.

- > **Reporte de preventivos y siniestros:** Se refiere a una cultura de prevención y anticipación del delito, mediante la cual la empresa reporta información e integra la oferta de servicio a nivel nacional donde haga presencia de negocio en apoyo a la Investigación Criminal (10/100).



- > **Suministro de denuncias:** Hace referencia al suministro oportuno y personal por parte de la empresa, de las denuncias en las que se actúe como interviniente procesalmente en el ámbito penal o control y vigilancia administrativa (10/100).

- > **Capacitación para la prevención:** Asistencia personal a las convocatorias de entrenamiento en prevención de delitos que lidera el programa FSE DIJIN, e implementación de un plan interno, que desarrolle un cronograma anual de entrenamiento en prevención, disuasión y desestimulación de delitos, dirigido a su personal, internamente. La cual se pondera convocatorias sobre número de asistencias en el año de la vigencia (10/100), y envío semestral del plan anual de capacitaciones para la prevención y anexos de evidencias documentadas de entrenamientos realizados (05/100).



- > **Asistencia a Mesas Técnicas Sectoriales:** Asistencia personal por parte del responsable FSE o delegación por escrito, a las convocatorias de este escenario por parte del FSE DIJIN, la cual se pondera número de convocatoria frente a número de asistencias con base en la última actividad realizada (05/100).

- > **Suministro de Información:** Este ítem está reservado de manera exclusiva a las empresas que por conducto del FSE DIJIN suministren información efectiva, que haya permitido la desarticulación de una organización delictiva (10/100).



- > **Actualización de Documentos:** La empresa debe renovar anualmente la documentación que acredita su constitución legal y funcional, en ella recae la responsabilidad de mantener activos los canales que garanticen las comunicaciones con el programa (Certificado de Cámara de Comercio, Licencia de Superintendencias, Certificado de no sanciones, dirección de la sede, correos corporativos, celulares y teléfonos de contacto); para tales efectos el FSE envía diariamente Boletines de Novedades, invitaciones y comunicados de interés, que el responsable FSE en la empresa asume el compromiso de difusión y garantiza su diaria recepción, reportando cualquier novedad a los canales de comunicación ampliamente difundidos por el programa (10/100).

- > **Cultura Estudios de Confiabilidad:** La empresa deberá reportar semestralmente las medidas adoptadas, en materia de estudios de confiabilidad, dirigido a personas naturales y jurídicas con las que sostenga vínculos laborales y comerciales en el ámbito de selección y mantenimiento posterior (10/100).



- > **Certificación en sistemas de Gestión (seguridad en procesos y procedimientos):** Ítem reservado a fomentar la implementación acreditada de buenas prácticas, como compromiso y corresponsabilidad empresarial, con la calidad del servicio prestado, insumo fundamental en la mitigación de riesgos asociados a la comisión de delitos. (Envío oportuno de la copia de certificaciones y/o recertificaciones) (10/100).

- > **Participación en la Flota de Avantel:** Participación y apoyo solidario en el canal grupal del FSE flota 123 grupo 2. (Nivel de participación por comunicación grupal) (10/100).



- > **Asistencia a Encuentro Anual:** Escenario destinado a la convocatoria exclusiva de Representantes Legales inscritos en Cámara de Comercio de las empresas vinculadas al programa: Asistencia de Representante Legal (10/100), Delegado con carta de justificación por parte de delegado (05/100).

Eventos Frente Seguridad Empresarial



3.3 Otras capacidades de apoyo a los empresarios Red Integral de Transporte



3.1.1 Red de apoyo - Dirección de Seguridad Ciudadana

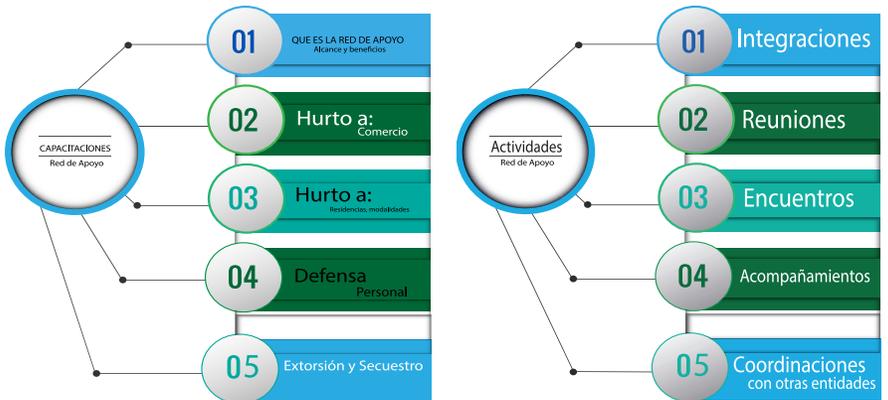
Conjunto de medios de comunicación y recursos humanos, organizados, canalizados y liderados por la Policía Nacional, con el fin de captar la mayor cantidad de información, para prevenir la comisión de delitos y contravenciones que afectan la tranquilidad y convivencia ciudadana.

Proceso para vincularse

1. Radicar la solicitud junto con los formatos anexos "requisitos"
2. Verificación de documentación
3. Estudio de confiabilidad "sipol"
4. Firmar acta de vinculación
5. Asignar un indicativo
6. Realizar una charla sobre el funcionamiento de la Red de apoyo.



Portafolio de servicios



Beneficios

El ciudadano, una vez vinculado a la red de apoyo previo a los documentos solicitados, recibe una capacitación sobre la utilización del medio y el alcance policial con que cuenta la institución en las diferentes áreas y especialidades, con el fin de utilizarlas las 24 horas, los siete días a la semana.



3.3.2 RISTRA Red Integral para el Transporte - Dirección de Tránsito y Transporte

¿Qué es el RISTRA?

La Red Integral de Seguridad en el Transporte de la Dirección de Tránsito de la Policía Nacional, busca fortalecer canales de comunicación con los diferentes actores de la cadena de suministro, contribuyendo a la prevención de los riesgos asociados a la seguridad en el transporte, como usuarios de la red vial nacional, nace con la Directiva Administrativa 0029 del año 2011 emanada por el Ministerio de Defensa Nacional.

Objetivo

Fortalecer los canales de comunicación con los actores de la cadena de suministro.

Líneas de atención RISTRA 24/7:

Atención requerimientos, suministro de información, al servicio de los actores de la cadena de suministro.

Avanteles: 13*7075 - 123*796

Celulares: 311-2899488 - 318-5509658

Ministerio de Transporte - Avenida El Dorado CAN entre Carreras 57 y 59 (Bogotá, D.C - Colombia).

Dirección de Tránsito y Transporte Policía Nacional Calle 13 No. 18-24.

Correos electrónicos: ditra.ristra@policia.gov.co

Líneas de Acción:

Transporte de Carga

Hidrocarburos y Sustancias Peligrosas

Operación Especial por Medidas Especiales

Carga Refrigerada

Operadores Postales

Transporte de Pasajeros
Transporte de Valores
Generadores de Carga
Operadores Logísticos
Agentes de Carga Internacional
Empresas de Localización Monitoreo y Tecnología afines
Agremiaciones de Transporte
Servicios Complementarios.

Productos y servicios

- **Boletín Informativo RISTRA**
- **Verificación protocolos empresariales de seguridad en el transporte:**
Se realiza verificaciones a procesos de seguridad con el fin de detectar rupturas o incumplimientos en la aplicación
- **Planes de disuasión internos en las empresas:** previa solicitud de las empresas inscritas a la red, en sus instalaciones se realizan planes de verificación de requerimientos y/o antecedentes judiciales.
- **Entrenamientos empresariales en seguridad en el transporte:**

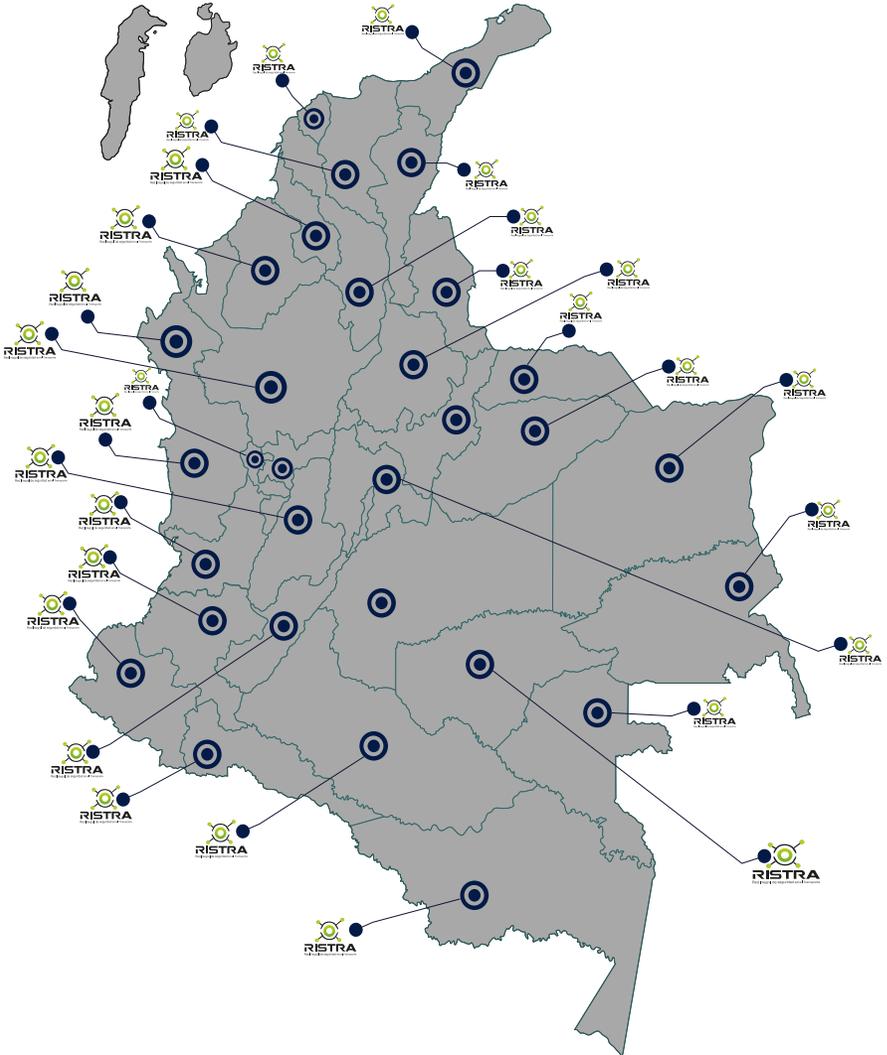
Modalidades Delictivas en el Hurto de Mercancías.

Riesgo Público (Modus Operandi del Hurto).

Detección y Control de Paquetes Sospechosos.
Identificación y Detección de Documentos Falsos.
Técnicas de Inspección en Contenedores de Carga.
Técnicas de Identificación Marcaria de Automotores.
Identificación de Caletas (Contaminación de la carga).
Transporte Internacional Operaciones Logísticas Seguras.
Búsqueda y Análisis de la Información.
Seguimiento Control Tráfico.

Cobertura:

A través de las Unidades Básicas de Investigación Criminal DITRA de las Seccionales de Tránsito y Transporte en el país.





3.3.3 Programa Yo no pago, Yo denuncio - Dirección Antisecuestro y Antiextorsión

Oferta Preventiva

Jornadas

Actividades direccionadas a los diferentes segmentos poblacionales de la comunidad, las cuales obedecen a una planeación, buscando generar recordación y fortalecer la cultura de autoprotección y autorregulación ciudadana frente al secuestro y la extorsión. Son ejecutadas a través de actividades de **(comunicación interpersonal, radial, prensa escrita, televisión, entre otras)**.



Conferencias

Actividades dirigidas a representantes de los diferentes gremios y comunidad en general, para tratar asuntos de índole preventivo frente al secuestro y la extorsión. Se realizan apoyados en una presentación básica sobre las principales modalidades de secuestro y la extorsión, estructura delincencial, modus operandi, autores delincuenciales y medidas preventivas.

Alianzas Estratégicas

Son acuerdos entre dos o más personas naturales y/o jurídicas, quienes de manera corresponsable articulan esfuerzos con el GAULA de la Policía Nacional de Colombia, para el desarrollo de acciones comunes que permitan minimizar riesgos y amenazas frente a los delitos de secuestro y extorsión.

Recomendaciones En el lugar de trabajo

- Conozca bien a sus compañeros de trabajo.
- Instale sistemas de seguridad que permitan controlar los puntos vulnerables de su empresa.
- Incremente las medidas de seguridad al ingresar o salir de su sitio de trabajo.
- Cambie la ruta de llegada y salida de su empresa u oficina, evite la rutina.
- Informe sus desplazamientos a una empresa de confianza.
- Nunca lleve consigo grandes cantidades de dinero.



En sus desplazamientos

- Cuando realice largos trayectos procure hacerlo por vía aérea.
- Capacite constantemente a su personal para que reaccione eficazmente ante un inminente peligro.
- Cambie la ruta de llegada y salida de su empresa u oficina, evite la rutina.
- Consulte a la Policía de Carreteras el estado de las vías antes de viajar.
- En lo posible, no viaje de noche.



Riesgos al pago económico por Secuestro y/o Extorsión

- No garantiza el regreso de la víctima sana y salva a la libertad.
- Aumenta el riesgo de un nuevo secuestro y aumento de extorsiones a su familia.
- Fortalece al delincuente y lo estimula a continuar realizando secuestros y extorsiones.
- Termina con su tranquilidad y la de su familia.
- Continúan con las exigencias hasta dejarlo en la quiebra después de que usted realice el primer pago.
- Recuerde, no acceda ante las presiones, si paga no terminarán las amenazas.





Con sus empleados

- Al contratar personal verifique todos sus antecedentes laborales y judiciales.
- Imparta instrucciones precisas y entrénelos sobre la forma de contestar el teléfono, la información que “no” debe suministrar y las frecuentes llamadas falsas con suplantación de voces.
- Procure que las joyas, el dinero y otros valores no permanezcan al alcance de los empleados.
- Evite informar con anticipación sobre horarios de viaje, posibles paseos o vacaciones de la familia.
- Si la empleada queda al cuidado de la casa, dé instrucciones precisas sobre el no ingreso de familiares y amigos.
- Exija que siempre verifique quién ha llegado antes de abrir la puerta, bien sea desde una ventana, un segundo piso, el visor o un sitio que lo permita.
- Repita con frecuencia toda la instrucción recomendada en esta guía; tenga presente que las empleadas y los niños, son más vulnerables al engaño y a la manipulación, y por esta razón fallan en las medidas de seguridad.



3.3.4 Programas de prevención - Dirección Antinarcóuticos

La Dirección de Antinarcóuticos cuenta con programas y campañas de prevención integral, dentro de un sistema criminal de narcotráfico que requiere tener como cobertura los siguientes blancos, así:

La Producción: En el cual se desarrollan campañas psicosociales, “Brigadas Médico - Quirúrgicas, Ferias sociales”, intervenciones focalizadas en municipios con concentración de cultivos ilícitos, programa frente a los comportamientos asociados a la siembra de cultivos ilícitos.

El Tráfico: Programa de prevención frente al tráfico de drogas, bus interactivo.

Distribución y Comercialización: Programa de escolarizado de prevención, bus interactivo, ciudadela de prevención, campañas de buen uso del tiempo libre, talento y folclor colombiano.

Esta Dirección cuenta con **118** instructores en prevención al consumo de drogas, distribuidos en 12 compañías Antinarcóuticos a nivel nacional.

Para la ejecución de las acciones se derivan diferentes estrategias, en total se cuenta con **11** ciudadelas de Prevención, **4** Buses interactivos, **9** personajes virtuales, **5** Saltarines.

El proceso que se adelanta es “Desarrollar estrategias educativas para la prevención en la oferta y demanda de las drogas”.

El programa bandera es el programa escolarizado de prevención basado en la evidencia:

EDAD	PROGRAMA	No. LECCIONES	OBJETIVO	DURACIÓN
5- 6	Aprende jugando	5	Identificación de riesgos básicos	5 semanas
7- 8	Aprende a valorarte	5	Crear bases de convivencia	5 semanas
9- 11	Educación y Prevenir	10	Aplicación del Modelo de Toma de Decisiones frente a los daños ocasionados por el consumo de drogas.	1 Trimestre
12- 14	Toma el control de Tu Vida	10	Concientización de las responsabilidades sociales y legales	1 Trimestre
15-18	Bachillerato	10	Reconocer y aprender a manejar los sentimientos de enojo sin recurrir a la violencia o al uso de alcohol y drogas.	1 Trimestre
Padres	Educación para Padres	5	Responsabilidad compartida (Policía- Padres y estudiantes)	5 Semanas

4

CAPÍTULO



Marco Normativo



Consejo NACIONAL
DE POLICÍA Y
CONVIVENCIA
Para *vivir* en paz

4. MARCO NORMATIVO

166

4.1 Requisitos legales aplicables a algunos actores de la cadena de suministro

Normatividad Sector Vigilancia y Seguridad Privada normas	
Norma	Descripción
Ley 734	Por la cual se expide el Código Disciplinario Único.
Ley 61	Por la cual se reviste al presidente de la república de facultades extraordinarias para dictar normas sobre armas, municiones y explosivos, y para reglamentar la vigilancia y seguridad privadas.
Ley 62	Por medio la cual se expide normas sobre la Policía Nacional, se crea la superintendencia de Vigilancia y Seguridad Privada.
Decreto ley 356	Por la cual se expide el estatuto de vigilancia y seguridad privada.
Ley 1119	Por la cual se actualizan los registros y permisos vencidos para el control al porte y tenencia de las armas de fuego y se dictan otras disposiciones.
Ley 1151	Por la cual se expide el Plan Nacional de Desarrollo.
Ley 1539	Por medio de la cual se implementa el certificado de aptitud psicofísica para el porte y tenencia de armas de fuego y se dictan otras disposiciones.
Ley 1712	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Normatividad Sector Vigilancia y Seguridad Privada Decretos	
Norma	Descripción
2535	Se expiden normas sobre armas, municiones y explosivos
1809	Por el cual se reglamenta el Decreto 2535/93.
619	Se reglamenta el artículo 31 del Decreto Ley 2535/93
356	Estatuto de Vigilancia y Seguridad Privada
2974	Se reglamentan los servicios especiales y comunitarios de vigilancia
1470	Se reglamenta el artículo 100 del decreto extraordinario 2535/93.
2187	Se reglamenta el estatuto de vigilancia decreto-ley 356/94.
1979	Uniformes y equipos para el personal de los servicios de vigilancia.
3222	Se reglamenta parcialmente el estatuto de vigilancia y seguridad privada

Norma	Descripción
1612	Modifica y adiciona parcialmente el decreto 2974/97, servicios comunitarios.
73	Tarifas mínimas para el cobro de los servicios de vigilancia
71	Cuantías mínimas de patrimonio de los servicios de vigilancia.
2355	Estructura de la SuperVigilancia
2356	Modifica la planta de personal de la Supervigilancia.
4950	Por la cual se fijan las tarifas mínimas para el cobro de los servicios de vigilancia
1989	Por el cual se reglamenta el pago de la contribución
503	Por el cual se modifica parcialmente el Decreto 2858 del 27 de julio de 2007.
2885	Por el cual se modifica el artículo 34 del Decreto 2187 de 2001
2368	por el cual se reglamenta parcialmente la Ley 1539 de 2012 y se dictan otras disposiciones
934	Que modifica el Artículo 8 del Decreto 0738 de 2013 (ampliación plazo examen psicofísico)
038	Por medio del cual se establecen medidas para la circulación de vehículos automotores el día 5 de febrero de 2015 y se dictan otras disposiciones.

Algunas normas aplicables a todos los sectores en Colombia

Norma	Descripción
Ley 30	Por la cual se adopta el Estatuto Nacional de Estupefacientes y se dictan otras disposiciones.
Ley 733 de 2002	Por medio de la cual se dictan medidas tendientes a erradicar los delitos de secuestro, terrorismo y extorsión, y se expiden otras disposiciones.
Ley 1028	Por la cual se adiciona el Código Penal y se dictan otras disposiciones- "Del apoderamiento de los hidrocarburos, sus derivados, biocombustibles o mezclas que los contengan y otras disposiciones".
Ley 1121	Por la cual se dictan normas para la prevención, detección, investigación y sanción de la financiación del terrorismo y otras disposiciones.
Ley 1273	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1453	Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad.
Ley 1480	Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones.
Ley 1581	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1762	Por medio de la cual se adoptan instrumentos para prevenir, controlar y sancionar el contrabando, el lavado de activos y la evasión fiscal.

Algunas normas aplicables a todos los sectores en Colombia

Norma	Descripción
Decreto 174 de 2006	Secretaría de Tránsito y Transporte Por medio del cual se adoptan medidas para reducir la contaminación y mejorar la calidad del Aire en el Distrito Capital. Aplica: Todas
Resolución 5776 de 2007	Ministerio de Transporte Por la cual se establecen unas medidas de tránsito vehicular tendientes a garantizar la movilidad en las vías del país. Aplica: Transportadoras de carga
Resolución 2307 de 2014	Ministerio de Transporte Por la cual se establecen medidas para la regulación del tráfico vehicular tendientes a garantizar la movilidad en las vías del país y se dictan otras disposiciones. Aplica: Transportadoras de carga
Resolución 9696 de 2003	Ministerio de Transporte Por la cual se establecen los requisitos técnicos de seguridad para los dispositivos especiales de sujeción de contenedores de acuerdo con lo establecido en el artículo 32 de la Ley 769 de 2002. Aplica: Todas
Resolución 2394 de 2009	Ministerio de Transporte Por la cual se dictan unas disposiciones en materia de seguridad. Aplica: Todas
Circular 010 de 2012	Superintendencia de Puertos y Transporte Solicitud Información Financiera - VIGIA. Aplica: Transportadoras de carga
Decreto 1609 de 2002	Por el cual se reglamenta el manejo y transporte terrestre automotor de mercancías peligrosas por carretera.
Resolución 1401 de 2012	Por la cual se señala el criterio para definir la autoridad ambiental competente para aprobar el plan de contingencia del transporte de hidrocarburos o sustancias nocivas de que trata el inciso 2 del artículo 3o del Decreto 4728 de 2010.
Resolución 315 de 2013	Ministerio de Transporte Por la cual se adoptan unas medidas para garantizar la seguridad en el transporte público terrestre automotor y se dictan otras disposiciones. Aplica: Transportadoras de carga
Resolución 377 de 2013	Ministerio de Transporte Por la cual se adopta e implementa el Registro Nacional de Despachos de Carga, RNDC. Aplica: Generador de carga
Circular 22 de 2013	Superintendencia de Puertos y Transporte Cumplimiento a la resolución 377 de 2013 - RNDC. Aplica: Generador de carga
Circular externa 014 de 2014	Superintendencia de Puertos y Transporte Cumplimiento de la normatividad relacionada con el Programa de control y seguimiento a las infracciones de tránsito de los conductores de las empresas de servicio público. Aplica: Transportadoras de carga

Normatividad Sector Transportadores de carga

Norma	Descripción
Resolución 5081 de 2006	Por la cual se fija el procedimiento administrativo para la inscripción en el Registro de los Operadores de Transporte de Carga Extradimensionada y se adopta el formulario para su trámite.
Ley 769 de 2002	Por la cual se expide el Código Nacional de Tránsito Terrestre y se dictan otras disposiciones
Acuerdo 051 de 1993	Ministerio de Transporte Equipo de carretera.
Resolución 1384 de 2010	Ministerio de Transporte Por la cual se adopta el método para establecer los límites de velocidad en las carreteras nacionales, departamentales, distritales y municipales de Colombia.
Ley 1548 de 2012	Secretaría General Por la cual se modifica la Ley 769 de 2002 y la Ley 1383 de 2010 en temas de embriaguez y reincidencia y se dictan otras disposiciones.
Decreto 390 de 2016	Por el cual se establece la regulación aduanera.
Decreto 2685 de 1999	Por la cual se modifica la legislación aduanera

Transporte multimodal y transporte internacional Acuerdo de Cartagena

Norma	Descripción
Decisión 290 de 1991	Se aprueba la Póliza Andina de Seguro de Responsabilidad Civil para el Transportador Internacional por Carretera y el Anexo que ampara Accidentes Corporales para los Tripulantes Terrestres Aplica: Transportador internacional
Decisión 393 de 1996	Transporte Multimodal Aplica: Todos
Decisión 331 de 1997	Transporte Multimodal Aplica: Todos
Decisión 399 de 1997	Transporte internacional de mercancías por carretera. Aplica: Transporte internacional
Decisión 467 de 1999	Se establecen las infracciones y el régimen de sanciones para los transportistas autorizados del transporte internacional de mercancías por carretera. Aplica: Transporte internacional

Transporte multimodal y transporte internacional Acuerdo de Cartagena	
Norma	Descripción
Decisión 491 de 2001	Reglamento Técnico Andino sobre Límites de Pesos y Dimensiones de los Vehículos destinados al Transporte Internacional de Pasajeros y Mercancías por Carretera. Aplica: Transporte internacional
Decisión 617 de 2005	Tránsito aduanero comunitario. Aplica: Transporte comunitario

Transporte multimodal y transporte internacional Ministerio de Hacienda y Crédito Público	
Norma	Descripción
Decreto 2685 de 1999.	Por la cual se modifica la regulación aduanera
Decreto 390 de 2016	Por la cual se establece la regulación aduanera
Actor que le aplica:	Usuario operador de zona franca, Agente de carga y transportador

Transporte de mercancía peligrosa, hidrocarburos y sustancias controladas	
Norma	Descripción
Decreto 321 de 1999	Ministerio del Interior Por el cual se adopta el Plan Nacional de Contingencia contra derrame de hidrocarburos, derivados y sustancias nocivas. Aplica: Generador de carga y transportador de carga
Decreto 1609 de 2002	Ministerio de Transporte Por el cual se reglamenta el manejo y transporte terrestre automotor de mercancías peligrosas por carretera. Aplica: Transportador de carga
Decreto 4299 de 2005	Ministerio de Transporte Por el cual se reglamenta el artículo 61 de la Ley 812 de 2003 y se establecen otras disposiciones. Aplica: Transportador de carga
Resolución 181682 de 2005	Ministerio de Minas y Energía Por la cual se adopta el Reglamento para el Transporte Seguro de Materiales Radiactivos. Aplica: Todos

4.2 Nuevo Código Nacional de Policía y Convivencia, Ley 1801 del 29 de julio de 2016



El Nuevo Código es un instrumento normativo de la mayor importancia para la nación, que más allá de ser una herramienta del poder de Policía, sin duda alguna es un instrumento para la paz, la convivencia armónica y la seguridad ciudadana de todos los colombianos; los cambios y transformaciones de una sociedad también cobijan a sus empresarios.

La palabra código deriva de diferentes términos del latín que guardan relación con los códigos o libros en madera donde los romanos escribían sus reglas. Los códigos se construyen, entre otras razones, para orientar el comportamiento humano.

En este sentido, las normas de policía son por excelencia los códigos de conducta de una sociedad que respeta los derechos de las personas y que vive en una sana convivencia. Igualmente, son instrumentos que buscan corregir aquellos comportamientos que afectan las buenas relaciones entre las personas y el entorno que las rodea. Por eso, la aprobación de este Código, por parte del Congreso de la República, constituye un elemento fundamental que prepara a la Policía y a la comunidad para el posacuerdo.

El nuevo Código no establece “contravenciones de policía” y, en su remplazo, introduce el término “comportamientos contrarios a la convivencia”, frente a los cuales impone “medidas correctivas”.

Estas normas son de carácter preventivo y por lo tanto no sancionan, solo corrigen comportamientos y buscan fomentar las buenas conductas por parte de las personas que se encuentran en el territorio nacional.

Tomado del artículo “Una herramienta para la construcción de la paz”, del volumen 307 Revista Policía Nacional

Finalidad

- Es un instrumento para la paz y la convivencia
- Tiene carácter preventivo y no represivo
- Es un código de los ciudadanos, las autoridades administrativas y civiles
- Previene y evita que problemas de convivencia se conviertan en asuntos penales
- Promueve la interacción pacífica y respetuosa
- Los comandantes de Estación y los Inspectores de Policía son actores fundamentales en esta ley
- Garantiza los derechos y libertades
- Significativo avance en la calidad de vida
- Permite actuar en forma inmediata
- Cuenta con veeduría ciudadana
- Regula el comportamiento en espacios públicos

Convivencia y comportamientos contrarios

Este compendio normativo contempla más de 300 comportamientos contrarios a la convivencia, en procura de encontrar el equilibrio armónico entre los que se destacan:

- Vida e integridad
- Tranquilidad y relaciones respetuosas
- Espacio público y movilidad
- Comportamientos que afectan relaciones entre personas
- Convivencia en sistema de transporte
- Seguridad en servicios públicos
- Relaciones respetuosas con grupos específicos
- Derecho a la reunión
- Recursos hídricos, fauna, flora y aire
- Basuras residuos y escombros
- Relaciones con animales
- Artículos pirotécnicos y sustancias peligrosas
- Establecimientos educativos

20

Aspectos importantes del nuevo Código Nacional de Policía y Convivencia

Para la sociedad y construcción de la cultura ciudadana



- 1 Control y manejo de basuras
- 2 Amenaza con causa daño físico por cualquier medio
- 3 Porte de elementos o sustancias peligrosas
- 4 Porte de armas neumáticas – aire – foguero – spray
- 5 Daño o no reparación de redes de servicio público
- 6 Prender fuego en espacio publico, quemas o incendios
- 7 Manipulación , conservación y manejo de artículos pirotécnicos
- 8 Regulación e intervención fuentes de ruido
- 9 Acto sexual o exhibicionismo en espacio público
- 10 Fumar en lugar prohibido
- 11 Consumo de alcohol o sustancias psicoactivas en colegios o entornos
- 12 Fortalece el principio de autoridad
- 13 Empleo indebido de líneas de emergencia
- 14 Prelación Adulto mayor - mujeres en gestación – niñas , niños y adolescentes
- 15 Derecho a reunión e irrespeto a manifestación
- 16 Uso de baños en establecimientos públicos Adulto mayor - mujeres en gestación – niñas , niños y adolescentes
- 17 Transporte de perros sin bozal – pólizas – peleas de caninos prohibidas como espectáculo – censo – omitir recoger excremento
- 18 Hacer necesidades en espacio público
- 19 Ingreso o salida de sistema de transporte público por puerta no autorizada - forzar puertas
- 20 Implementar cámaras de vigilancia en transporte masivo

¿Para qué le sirve el CNPC al ciudadano?

174

> En materia de respeto por la integridad del espacio público y los bienes culturales

Los grafitis en lugares públicos o abiertos al público, postes, fachadas, antejardines, muros, paredes, bienes culturales, solo podrán realizarse en zonas que se encuentren habilitadas para esta expresión artística.

> La ley no proscribire los grafitis como expresión artística

Lo que hace es establecer que los mismos, se podrán llevar a cabo en zonas habilitadas y previo permiso de la autoridad competente.

> En materia de comercialización de equipos celulares

Sólo podrán comercializar equipos celulares quienes tengan la autorización expedida por el Ministerio de Tecnologías de la Información.

> En materia de apertura de establecimientos comerciales y respeto a las normas del uso del suelo.

La apertura de cualquier establecimiento debe informarse con anterioridad al Comandante de Estación o Subestación de Policía.

> En materia de normas tendientes a preservar la convivencia en medios e instalaciones del servicio público de transporte.

A quien manipule, deteriore, destruya o bloquee las puertas de las estaciones u ocasione daño a los buses articulados del sistema masivo de transporte.

> En materia de protección a los animales

Protege a las mascotas y habilita para que la autoridad de policía de manera inmediata corrija a los dueños de mascotas que no cumplan con las normas de convivencia.

> En materia de manejo de basuras

En los casos de mal manejo de residuos o basuras, la autoridad de policía podrá intervenir de manera inmediata para corregir este comportamiento mediante la imposición de comparendos.

> Impulsar el respeto a la autoridad

Se impondrán medidas correctivas ejemplarizantes a quien irrespete a la autoridad de Policía o incumpla, desacate, desconozca o impida la función o la orden de Policía.





“Haga parte del Frente de Seguridad Empresarial de la Policía Nacional, esta es una red de prevención criminal a nivel nacional e internacional, que le permite comunicación permanente con autoridades y acceso a las capacidades institucionales, impactando la gestión del riesgo de la empresa, así como su interacción en las cadenas de valor”.

Mayor Gelga Buitrago Martínez

Jefe Área Asistencia y Cooperación para la Policía Judicial, Frenes de Seguridad Empresarial