DIJIN

HERRAMIENTA DE SEGURIDAD PARA LOS ACTORES DE LA CADENA DE SUMINISTRO

PAUTAS PARA LA PREVENCIÓN CRIMINAL

VI EDICIÓN

2019

VI Edición

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

Herramienta de Seguridad para los actores de la Cadena de Suministro

Pautas para la prevención criminal

2019

Ministerio de Defensa Nacional
Policía Nacional de Colombia

ISBN 978-958-98894-7-3

VI Edición

General
Óscar Atehortúa Duque
Director General Policía Nacional

Mayor General
Gustavo Alberto Moreno Maldonado
Subdirector General Policía Nacional

Mayor General
Fabio Hernán López Cruz
Director de Investigación Criminal e INTERPOL

Coronel
José Libardo Restrepo Villamil
Subdirector de Investigación Criminal

Coronel
Henry Ramírez Ramírez
Jefe de Investigación Judicial

Teniente Coronel
Cenide Carolina Rodríguez Paz
Jefe Área Asistencia y Cooperación para Investigación Judicial

Mayor
Andrea del Pilar Díaz Rodríguez
Jefe Frente de Seguridad Empresarial

Corrección de Estilo
Nelson A. Rojas Vargas

Diseño, diagramación e impresión
Fenix Media Group S.A.S.
Bogotá, D. C., Colombia, noviembre de 2019

AGRADECIMIENTOS

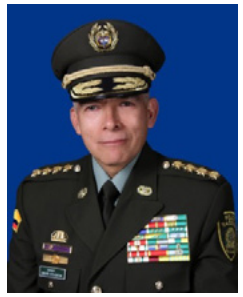
A todas las personas y entidades que realizaron su valioso aporte y contribución en la elaboración de la VI Edición de la Herramienta de Seguridad para los Actores de la Cadena de Suministro, que tiene como finalidad brindar un instrumento práctico al sector productivo de bienes y servicios, para contribuir a la prevención criminal mediante el fortalecimiento de la gestión del riesgo y la prevención en seguridad, impactando positivamente las diferentes unidades económicas mencionadas.

A los integrantes del Comité Editorial, que aportaron, redactaron y consolidaron el contenido de este documento: a la señora Teniente Coronel Cenide Carolina Rodríguez Paz, Jefe Área de Asistencia y Cooperación para Investigación Judicial de la DIJIN; a la señora Mayor Andrea del Pilar Díaz Rodríguez, Jefe Frente de Seguridad Empresarial; a la señorita Teniente Luz Amparo Pinto Rivera, Gestora de Seguridad Empresarial de la DIJIN; a la doctora Lina María Chacón Cancino, Gerente General INIF; al doctor Carlos Ariza Mora, Consultor Internacional en Seguridad Privada; al Ingeniero Jhon Jairo Mónoga, Auditor Internacional de BASC; al doctor Jairo Andrés Rodríguez Guerrero, Director General Grupo OET; al señor Teniente Coronel (RA) Eduardo Moreno Peláez, Auditor Internacional de BASC; al señor Coronel (RA) Fredy Bautista García, Experto en Ciberseguridad, y al señor Mayor (RA) Carlos Alfonso Boshell Norman, Subgerente Implementación Sistema de Administración Riesgos LA/FT, Superintendencia y Sector de la Vigilancia y Seguridad Privada. Julián Andrés Puentes B, Auditor y Docente del Sistema de Gestión ICONTEC; Raúl Hernán Muriel Botero, Consultor en Seguridad; Eduardo Hernández Ruíz, José Angel Vidaña Meraz y Rosa María del Carmen Jiménez Mendoza, del Consejo de Seguridad en cadena de Suministro de México; Benjamín Grajeda Regalado y José Luis Vilchis Maya, de la Gendarmería Nacional de México.

En especial a BASC Bogotá, Cámara Colombiana del Libro, ICONTEC, INIF; al equipo de trabajo del Frente de Seguridad Empresarial y demás empresarios que realizaron su valioso aporte, sin el cual hubiera sido imposible elaborar la herramienta que hoy estamos presentando.

Tabla de contenido

PRÓLOGO



En Colombia, los policías hemos aprendido que la gobernanza exitosa de la convivencia y la seguridad ciudadana depende de una combinación virtuosa de cinco factores: el fortalecimiento político-institucional, el desarrollo socio-económico, la integración social, la generación de políticas asertivas y el auge de una cultura de la legalidad que facilite la denuncia del delito.

A partir de esta comprensión, hemos obtenido logros históricos frente a la reducción del delito, con un gran impacto a favor de la vida, el patrimonio y la prosperidad de nuestro país. Actualmente, el país registra la décima parte de los secuestros de hace 20 años. Pasamos de ser un país estigmatizado, a convertirnos en una nación líder en la lucha contra este flagelo y el de la extorsión, que exporta su conocimiento contra el crimen, en sus distintas modalidades, a otros países.

De hecho, la gestión de la convivencia ha significado un gran esfuerzo en la creación y consolidación de exitosos mecanismos de interacción social, como la Red de Participación Cívica y el Frente de Seguridad Empresarial, al permitirnos incrementar las potencialidades del desarrollo sostenible, gracias a las alianzas estratégicas con los sectores público y privado, para mitigar riesgos y amenazas a través de una mejor comunicación y coordinación con la Fuerza Pública, ante el clamor de una ciudadanía más exigente, que reclama resultados trascendentes y estrategias integrales, mediante la implementación del Plan de Choque "El que la hace la paga", así como el despliegue de sus fases consecuentes: "Más cerca del ciudadano" y "Construyendo seguridad", ante el deber de doblegar la criminalidad organizada y confrontar la dinámica delictiva.

Nuestra hoja de ruta está dada en el Plan Nacional de Desarrollo 2018-2022, "Pacto por Colombia, pacto por la equidad", para cumplir el propósito de incentivar un nuevo tiempo de aceptación de la norma, no como imposición sino resultado de un proceso de transformación social, a fin de generar una nueva estructura relacional que nos permita la concepción de estrategias, el debilitamiento de estructuras criminales y la articulación entre la Policía con distintos organismos y entidades territoriales.

Un contexto propicio para aportar al lanzamiento de la VI Edición de la Herramienta de Seguridad para los Actores de la Cadena de Suministro, con el fin de mitigar los eventos que impactan negativamente el desarrollo de sus actividades, debido a que tanto la Red de Participación Cívica, como el Frente de Seguridad Empresarial constituyen un canal excepcional de comunicación multipropósito para enfrentar a la delincuencia, abordar la prevención y atención de desastres y la movilización solidaria ante circunstancias que lo requieran, así como la alerta temprana de situaciones que los ciudadanos consideren potencialmente peligrosas.

De hecho, los diferentes actores de la cadena de suministro han aportado a la construcción de esta valiosa herramienta de consulta para fortalecer la prevención de la criminalidad, a partir de diagnósticos actualizados y perspectivas empresariales que permitan una adecuada gestión del riesgo, elaboración de planes de continuidad de negocio y el blindaje de la seguridad asociada a procesos de operación, personal, información, instalaciones y demás activos de una empresa, mediante la adopción de los sistemas SIPLAFT (Sistema de Prevención y Control para el lavado de activos y la financiación del Terrorismo) y SARLAFT (el Sistema de Administración del Riesgo para el Lavado de Activos y Financiación del Terrorismo), para contribuir a la construcción de un país más seguro y competitivo, acogiendo la sentencia del filósofo y economista inglés John Stuart Mill[1], según la cual: *"no existe una mejor prueba del progreso de una civilización, que la del progreso de la cooperación"*; una sinergia que en este caso está representada en la cooperación imponderable[2] con el sector empresarial, para generar las mejores condiciones de seguridad, desarrollo económico y social, desde las posibilidades y los distintos escenarios de acción que nos brindan los actores de la cadena de suministro.

General ÓSCAR ATEHORTÚA DUQUE
Director General de la Policía Nacional

[1] Filósofo, político y economista inglés de origen escocés, representante de la escuela económica clásica y teórico del utilitarismo.

[2] Insuperable o inmejorable.

INTRODUCCIÓN

La seguridad en la cadena de suministro es una parte importante, en la cual diferentes actores tienen responsabilidades y actividades que se deben cumplir, con el fin de garantizar que las operaciones de las compañías sigan su curso normal. Muchos de los programas corporativos de seguridad se basan en la experiencia de aquellos que los deben diseñar, implementar y administrar; sin embargo, dejamos de lado la importancia de entender claramente la base conceptual, y dejamos el diseño a partir de nuestra propia experiencia; por ello, con la ayuda de expertos de varias áreas queremos compartir con nuestros lectores pautas básicas y necesarias para que logren diseñar, mejorar, actualizar y poner en práctica todos los conocimientos, con el fin de contribuir a la mejora continua de nuestra seguridad empresarial.

Cuando se trata de controlar algo que se desconoce, se incurre en gastos de una forma innecesaria, con resultados que infortunadamente no son los esperados; por ello, se debe partir de la base de conocer la problemática que les rodea y estar actualizándose en la dinámica de las amenazas, las áreas en las que están presentes y los objetivos de mayor interés para eso; por lo anterior, antes de implementar medidas preventivas, lo primero que se debe hacer es detectar las amenazas que se encuentran en los entornos de operación, identificar las formas de delinquir, determinar los lugares en los que actúan los delincuentes y establecer si en verdad son o no un blanco atractivo para ellos. Eso significa tener percepción del riesgo real, lo cual es útil para establecer, proponer e implementar las contramedidas de seguridad adecuadas, para reducir la probabilidad de ocurrencia de incidentes, que no es otra cosa diferente a estar preparados para reducir el riesgo y minimizar el impacto de los hechos.

De otra parte, es importante mencionar que en muchas ocasiones se actúa solo; es decir, que no se tienen en cuenta otros actores, que pueden ayudar de manera directa y eficaz a revisar, identificar y prevenir los incidentes, y es allí donde las empresas o las instituciones de gobierno cobran mucha importancia; en ocasiones se es víctima de casos que no se comparten (la teoría de la lección aprendida), que sirven para mejorar la respuesta en caso de tener un incidente similar o que sirve a los demás para aprender con base en un evento real. Como institución del Estado, cuando se reporta un incidente de seguridad, se hace un análisis minucioso de él para poder identificar todas las variables que permitan realizar una investigación que arroje resultados satisfactorios, y que además genere conocimiento para el resto del gremio; por ello, dentro de esta publicación encontraremos los argumentos de varios expertos que buscan precisamente esto, generar el conocimiento para que los lectores puedan identificar cuáles de estos planteamientos les sirven para que vuelvan aún más robustos sus esquemas de seguridad en torno a la cadena de suministro.

En la lucha contra los delitos que afectan la cadena de suministro, se debe propender por el trabajo en equipo entre las instituciones, como la Policía Nacional, las agremiaciones privadas y los profesionales de la seguridad, pues lo que se busca es generar entornos de conocimiento para poder crear documentos como este, que sirvan de soporte para mejorar lo que se tiene o diseñar lo que se necesita. Se da una explicación muy simple y sencilla, en la que se abordan diferentes aspectos de la seguridad, pero además se busca con ello apoyar la gestión de todas aquellas personas que están encargadas de la seguridad, para que identifiquen las oportunidades de mejora en sus procesos y reduzcan la probabilidad de ocurrencia de incidentes que puedan afectar a sus organizaciones u operaciones.

De otra parte, desde el ámbito institucional se quiere mostrar a los lectores cómo a través de ser parte de los diferentes programas de prevención que tiene el gobierno, se pueden mejorar vínculos de asociación con equipos profesionales, que pueden dar soporte adecuado y oportuno cuando así se requiera. Desde nuestra institución se han venido gestando, promulgando, actualizando y compartiendo buenas prácticas de seguridad, que se han construido con el apoyo de agremiaciones privadas y de expertos en seguridad privada; lo anterior permite entregar, en esta nueva edición, información valiosa que servirá como consulta, con el fin de lograr la mejora continua en los procesos de seguridad de la cadena de suministro.

La institución está atenta a las necesidades de seguridad de un país pujante, ávido de obtener lo mejor de sus instituciones, y además establecer vínculos adecuados, fuertes y eficaces para prevenir el delito y crear acciones y actividades que permitan evitarlo; en caso de ocurrir esto, poder proporcionar una respuesta eficiente, mediante la creación de núcleos de trabajo y comunicación, en los que se analice la problemática y se puedan identificar responsables y modalidades de operación de las amenazas, con el fin de controlarlas a través de información oportuna.

Con el pasar de los años, el papel del sector público-privado en la prevención del delito ha recibido cada vez más atención; muchas empresas han adoptado estrategias para la prevención criminal, que se enfocan sobre lo que puede hacerse para impedir que el delito ocurra antes de la intervención del sistema penal acusatorio.

Una tendencia importante, que cobra relevancia en la participación del sector empresarial en la prevención criminal, ha sido la implementación de tecnologías de seguridad privada, para evitar pérdidas; este es un aporte en la reducción y prevención del delito: la georreferenciación del delito, los sistemas de circuitos cerrados de televisión, de alarma y vigilancia, tecnologías de reconocimiento facial y ocular, entre otros, son ejemplos de avances tecnológicos en la protección contra las pérdidas y en la disminución de eventos delictivos.

Por último, recordar que la responsabilidad social de la seguridad es de todos los actores que comparten el ambiente, y que cada uno de nosotros es parte

fundamental para poder detectar, prevenir y controlar el delito con la ayuda de las autoridades, a través del acercamiento y mantenimiento de lazos fuertes de unión, que permitan trabajar como un equipo efectivo para lograr que los colombianos convivan en paz.

Mayor General FABIO HERNÁN LÓPEZ CRUZ
Director de Investigación Criminal e INTERPOL

OBJETIVOS

General

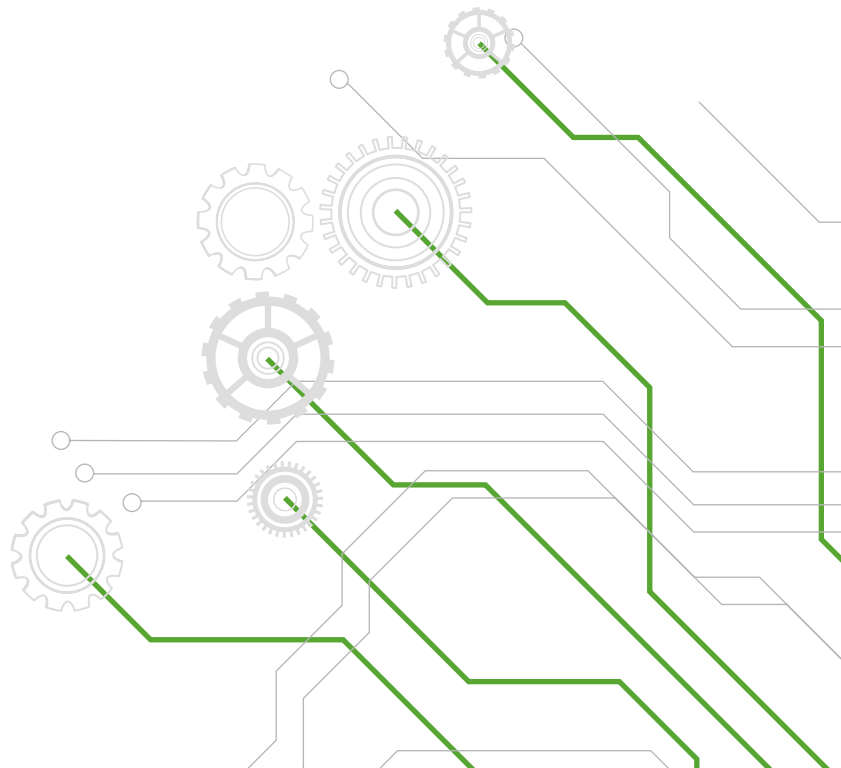
Dar a conocer a los diferentes integrantes de la cadena de suministro una herramienta práctica, que nos permita fortalecer el canal de comunicación multipropósito para enfrentar a la delincuencia, abordar la prevención criminal, atención de siniestros y la movilización solidaria ante circunstancias que lo requieran, así como la alerta temprana de situaciones que afecten la continuidad del negocio, siempre en cumplimiento de la misión y objetivos estratégicos institucionales.

Específicos

- Compartir información, para identificar en el contexto amenazas de seguridad a nivel global, regional y local.
- Fortalecer la articulación entre el sector productivo y el Frente de Seguridad Empresarial, en la construcción de escenarios de prevención que coadyuven en la continuidad del negocio en Colombia.
- Dar a conocer buenas prácticas en ciberseguridad a los empresarios en Colombia, que permitan controlar los eventos que impactan negativamente el desarrollo de sus actividades.
- Brindar al empresario una serie de actividades que promuevan la adopción de los sistemas SIPLAFT y SARLAFT dentro de la compañía.
- Ofrecer información que permita un mayor nivel de adaptación del sector privado a los retos y desafíos que impone la OCDE, con el fin de construir un país más competitivo.

CAPÍTULO 1

FRENTE DE SEGURIDAD EMPRESARIAL



1. Frente de Seguridad Empresarial

Objetivo

Apoyar a las empresas nacionales y extranjeras de cualquier sector empresarial para que garanticen la continuidad del negocio dentro de la cadena productiva, mediante el trabajo coordinado con la Policía Nacional, adoptando mejores procesos orientados a optimizar la seguridad de sus actividades, a través de la prevención, reacción y apoyo a la judicialización, con el fin de reducir la criminalidad que los afecta.

Frente de cobertura de negocios

Empresas de todos los sectores productivos en Colombia, pequeñas, medianas y multinacionales, que cumplan los requisitos de vinculación. Agrupadas en un modelo bifocal y multisectorial, así:agremiaciones (Cámara de Comercio, asociaciones, federaciones y confederaciones) transportadores, generadores de carga, operadores logísticos y demás actores de la cadena de suministro.

1. Organizaciones y empresas que luchan contra la falsificación de libros, videogramas y fonogramas, medicamentos, licor y autopartes.
2. Vigilancia y seguridad privada, administradores de riesgo, comunicaciones, seguimiento y monitoreo satelital.
3. Empresas de exploración y explotación de recursos naturales (petroleras y mineras).
4. Sector financiero, asegurador y transportador de valores.

Portafolio de servicios

Servicios sin costo, a los que acceden las empresas vinculadas, en reconocimiento y estímulo a la corresponsabilidad con la seguridad, de esta manera:

Jornadas de sensibilización: espacios inclusivos mediante convocatoria masiva, con los cuales se busca fortalecer la gestión de riesgos corporativos asociados a delitos, dirigida a los funcionarios de las empresas vinculadas, en las que se socializará la dinámica delictiva (modus operandi) para plantear medidas de mitigación y buenas prácticas, que permitan la detección temprana de amenazas que puedan afectar la continuidad de negocio.

Jornada de prevención sectorial: espacios de retroalimentación participativa por sectores similares de negocio, con el fin de fortalecer e implementar buenas prácticas de cultura de seguridad dentro del sector productivo participante.

Suministro de información de requerimientos judiciales de personas y vehículos: previo cumplimiento de consentimiento expreso del titular (Ley 1581 2012): la empresa podrá acceder a la consulta de requerimientos judiciales vigentes, para uso exclusivamente interno y soporte en la toma de decisiones.

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 la competencia de articular las capacidades de la Policía Nacional, de conformidad con la especificidad y jurisdicción de la necesidad en seguridad empresarial.

Boletines diarios informativos: difusión de información electrónica de recomendaciones en seguridad, buenas prácticas, resumen de noticias, novedades viales a nivel nacional, convocatorias a eventos de interés empresarial, entre otros.

Información estadística criminal: suministro de información estadística criminal, conforme con los tipos penales y modalidades delictivas registradas a nivel nacional y no sometidas a reserva, determinada por factores de tiempo, descripción geográfica y variables comparativas conforme a las especificaciones del requerimiento.

Asistencia y asesoría: orientación a las empresas de acuerdo con sus necesidades en materia de seguridad de sus procesos y/o afectación criminal.

Encuentro anual FESEM: 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.

Encuentros regionales FESEM: asistencia sin costo al evento anual por región, 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, nacional y/o regional en el manejo de temas inherentes a la seguridad empresarial.

Visitas de acompañamiento en campo: visitas aleatorias a las instalaciones de las empresas vinculadas, con el fin de afianzar la corresponsabilidad entre el sector público-privado con la seguridad ciudadana, brindando una respuesta acertada a la mitigación de los riesgos asociados a los procesos productivos.

Análisis criminológicos: suministro del comportamiento delictivo que afecta al sector productivo a nivel nacional y no sometido a reserva, determinado por factores de tiempo, descripción geográfica y variables comparativas, conforme a las especificaciones del requerimiento.

Análisis semestrales de ciberseguridad: difusión a las empresas vinculadas de las nuevas modalidades delictivas asociadas a la cibercriminalidad.

Herramientas de seguridad para los actores de la cadena de suministro: entrega trianual de pautas y recomendaciones, para contribuir a la prevención criminal fortaleciendo la gestión del riesgo y la seguridad, coadyuvando al cumplimiento de los objetivos estratégicos institucionales.

Requisitos de vinculación

ETAPA I

Inscripción

Formulario de inscripción, disponible en el sitio web del FESEM https://www.policia.gov.co/fse/vinculacion

Carta motivada dirigida al Jefe del Grupo FESEM o Jefe de la Seccional de Investigación Criminal de la correspondiente jurisdicción, firmada por el representante legal vigente inscrito en Cámara de Comercio, en la que otorgue consentimiento de estudio de seguridad y constancia de no tener en curso investigaciones o sanciones de tipo administrativo o penal en contra de la persona jurídica o sus socios.

Dos recomendaciones de empresas (escaneado PDF independiente) que gocen de reconocimiento público, con las que haya sostenido recientemente vínculos comerciales y con datos de contacto para validación.

Certificado Cámara de Comercio reciente (no superior a 30 días) y resolución de la superintendencia o ministerio que regula la actividad (solo si aplica) (escaneado PDF independiente).

ETAPA II

Visita técnica previnculación

La visita física a las instalaciones será realizada por el Gestor de Seguridad Empresarial, asignado por el FESEM, quien realizará el Acta de Reunión, plasmando los compromisos por parte del representante legal y el funcionario de la empresa delegado como representante ante el FESEM.

Criterios de visita técnica previnculación: validación de la existencia real de la empresa y la verificación de la política de seguridad integral corporativa, identificando oportunidades de fortalecimiento en la lucha contra la criminalidad e implementación de una cultura responsable y colaborativa con la Policía Nacional en la prevención y lucha contra los fenómenos delictivos que las victimizan en su operación.

ETAPA III

Vinculación

Se tramita mediante reunión, a la que asisten: representante legal, representante ante el Frente de Seguridad Empresarial, que ha superado el proceso de estudio de vinculación con el jefe del Frente de Seguridad Empresarial o Seccional de Investigación Criminal, gestor de seguridad empresarial, donde se socializarán ampliamente los beneficios y compromisos de las empresas vinculadas y se oficializará la vinculación a través de la firma del acta de vinculación.

Permanencia de las empresas vinculadas al FESEM

Se refiere a los compromisos que adquiere la empresa en su calidad de vinculada; será objeto de sustentación por parte del representante ante al FESEM, como requisito para la renovación de la vinculación en los eventos en que la empresa no evidencie una participación efectiva en el programa de prevención ofrecido a través del Frente de Seguridad Empresarial-DIJIN.

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, en apoyo a la investigación criminal.

Liderazgo participativo en corresponsabilidad: hace referencia a la iniciativa de acciones que promuevan y apoyen la gestión misional del programa de forma coordinada con el FESEM.

Compromiso para la prevención: asistencia del personal administrativo u operativo de las empresas a las convocatorias de entrenamiento en prevención de delitos, que lidera el programa FESEM-DIJIN, e implementación de un plan interno de entrenamiento en prevención, disuasión y desestimulación de delitos, dirigido al personal de su empresa.

Cultura de legalidad, ética y transparencia corporativa: prácticas empresariales que fomenten el buen actuar en el marco de la legalidad, lealtad de competencia, principios, valores corporativos, corresponsabilidad con la seguridad, que mitiguen el riesgo de incumplimientos mandatorios con consecuencias penales, administrativos y la ética de negocios.

Actualización de la información: la empresa debe renovar periódicamente la información 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 superintendencias, certificado no sanciones, representante ante el FESEM, dirección de la sede, correos corporativos, celulares, teléfonos de contacto u otros).

Cultura de estudios de confiabilidad y gestión del riesgo: la empresa deberá adoptar internamente procedimientos 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, al igual que la implementación de procedimientos en mejora continua y acciones encaminadas a la identificación, actualización, tratamiento y monitoreo de los riesgos de fuente criminal a su operación (prevención de la criminalidad que los afecta).

Certificación en sistemas de gestión (seguridad en procesos y procedimientos): 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 (certificaciones y/o recertificaciones).

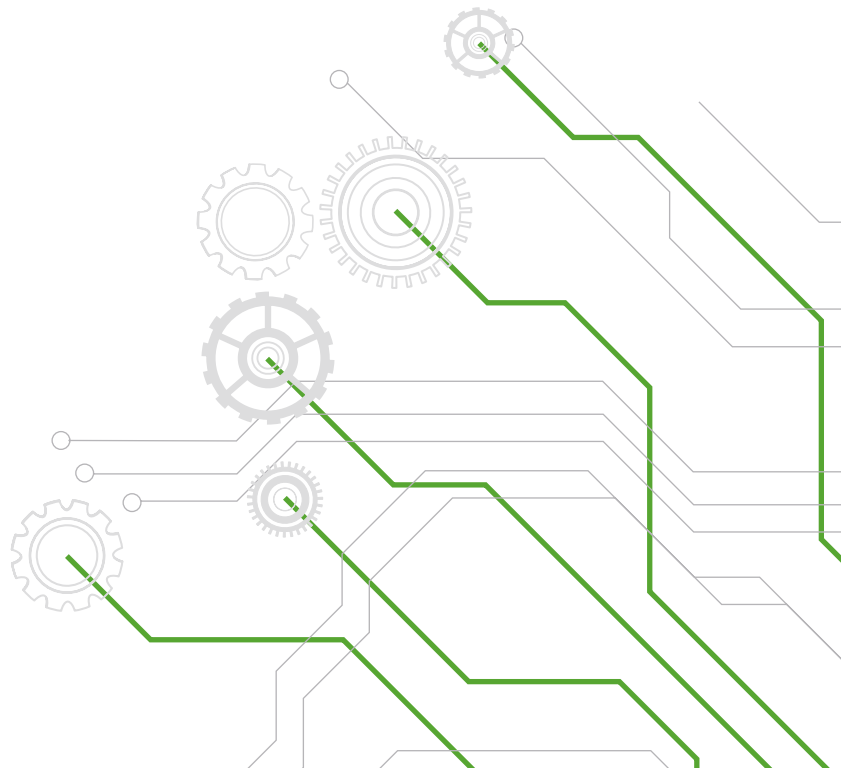
Participación en canales de comunicación grupal: activa participación en apoyo y solidaridad con las demás empresas vinculadas a los grupos de comunicación grupal, apoyados en los avances de la tecnología y comunicaciones disponibles, dispuestos para tal fin por el FESEM (correo electrónico, avantel, mensajería WhatsApp, otros).

Asistencia al encuentro anual: participar en el escenario destinado, mediante convocatoria exclusiva a los representantes legales de las empresas vinculadas al programa.

Todas las responsabilidades asistidas se deberán soportar mediante la utilización de los medios y metodologías archivísticas que se adecuen a su entorno, en donde se evidencie cada una de las actividades adelantadas, las cuales serán objeto de verificación y control como aporte a la convivencia y seguridad ciudadana.

CAPÍTULO 2

MARCO TEÓRICO DE LA SEGURIDAD PRIVADA



2. Marco teórico de la seguridad privada

Por: Lic. Ps. Carlos Ariza - Magíster en Criminología

Entre los nuevos retos que tiene el profesional de seguridad está el de diseñar y plantear esquemas de seguridad desde el punto de vista lógico y estratégico, para convertir el área de seguridad y protección en un aliado para el negocio. Muchos de nosotros siempre estamos a la espera de los requerimientos que nos hace el negocio o compañía, sin tener en cuenta que mucho de lo que ocurre o podría ocurrir forma parte del panorama de riesgos que debemos contemplar para poder ser el soporte adecuado en tiempo y forma cuando el negocio presenta interrupciones en sus operaciones. Para ello es importante que empecemos a entender que la seguridad está diseñada hace mucho tiempo, lo único que debemos es organizarla para crear la herramienta del Programa Corporativo de Seguridad, que será nuestro mapa para manejar adecuada y suficientemente todas esas situaciones que podrían afectarnos de manera directa o indirecta, y que de no ser detectadas a tiempo, podrían ocasionar daños y pérdidas que luego se convertirían en un problema prolongado y desgastante, que le costaría a la compañía dinero y recursos que podrían afectar la continuidad de la operación.

Para ello vamos primero a hablar de las variables que se deben tener en cuenta para poder estructurar un programa de seguridad adecuado, eficiente y eficaz, partiendo de la base de que cada programa debe ser costo-beneficioso para la compañía; por esta razón, no podemos recomendar implementar medidas de seguridad que estén por encima del activo que vamos a proteger; por lo tanto, debemos revisar los aspectos monetarios para así hablar de:

- ***ROI (por su sigla en inglés: Return of Invesment) - "Retorno de la inversión":*** que significa que a través de las inversiones de seguridad (equipos de seguridad electrónicos y activos), la gestión y la depreciación, en cuánto tiempo le regresaremos ese dinero al negocio y sobre qué indicadores vamos a medir que han sido efectivos.

- ***ROE (por su sigla en inglés: Return of Expense) - "Retorno del gasto":*** significa que a través de los gastos de seguridad (seguridad humana, escoltas, etc.) cómo vamos a mitigar los riesgos y reducir los impactos (mediante indicadores) de los gastos mensuales que se están pagando en seguridad.

Además, debemos empezar a comprender que para diseñar un programa lógico de seguridad es importante entender:

- Conceptos básicos de seguridad
- Modelos de seguridad más reconocidos

- Metodología de seguridad para diseñar e implementar el modelo corporativo de seguridad

Vamos a empezar por los modelos de seguridad, que para muchos son poco o nada conocidos desde lo conceptual; es decir, los conocemos porque los hemos implementado de alguna forma y nos han dado resultado, pero lo hemos hecho como parte de la herencia del conocimiento y de lo empírico. Estos modelos nos ayudarán a entender por qué y para qué nos sirven.

1. Modelo EASI *(por su sigla en inglés: Estimate of Adversary Sequence Interruption)* - Estimación de la Secuencia de Interrupción de los Pasos del Adversario: se busca identificar cómo estamos preparados en cuanto a seguridad física para reducir la probabilidad de una intrusión o un ataque directo; esto se logra realizando un adecuado análisis de riesgos y probando el sistema para poder identificar esas brechas con nada o poca cobertura, a través de ejercicios de pruebas de vulnerabilidad o penetración; desgraciadamente, nos damos cuenta de ello cuando se presenta un incidente de seguridad. Este modelo nos invita a identificar lo que tenemos ahora y cómo lo podríamos mejorar por medio de ejercicios en escenarios controlados, que nos ayudan a identificar:

a. Tenemos los controles adecuados
b. Tenemos los controles suficientes
c. Está el personal entrenado
d. El personal conoce lo que debe hacer
e. El control se lleva a cabo de manera permanente
f. El control lo aplican todos los involucrados
g. Se han realizado pruebas del control
h. Se han diseñado planes de acción para mejorar y actualizar el control

Lo que se busca con el modelo es identificar las vulnerabilidades del proceso de seguridad y mejorarlo mediante la realización de pruebas adecuadas y oportunas, para reducir la probabilidad de ocurrencia o el impacto en caso de que esto suceda, con el fin de crear esquemas de retardo y respuesta que generen disuasión en la intención de la amenaza.

Les compartimos una de las tablas utilizadas para poder llevar a cabo este tipo de ejercicios:

MATRIZ DE IDENTIFICACIÓN DE VULNERABILIDAD DE LOS SISTEMAS DE RESPUESTA							
CONTRAMEDIDA	ACCIÓN REALIZADA	TIEMPO QUE LE TOMA AL INTRUSO (Minutos)	TIEMPO DE ACTIVACIÓN DEL SISTEMA (Minutos)	ACCIÓN HUMANA DE SEGURIDAD	TIEMPO TOMADO (Minutos)	TIEMPO TOTAL DE LA RESPUESTA (Minutos)	NIVEL DE VULNERABILIDAD
Barrera Perimétrica de 8 pies sólida						0	0
Barrera Perimétrica de 8 pies en malla						0	0
Ventana con reja de protección						0	0
Ventana sin reja de protección						0	0
Puerta de seguridad						0	0
Puerta normal						0	0
Iluminación						0	0
Seguridad Humana						0	0
Seguridad canina						0	0
CCTV						0	0
Alarma perimetral						0	0

TIEMPO DE RESPUESTA	IMPACTO
DE 1 A 3 MINUTOS	Leve
DE 4 A 6 MINUTOS	Leve Bajo
DE 6 A 8 MINUTOS	Grave Bajo
DE 8 A 10 MINUTOS	Grave
DE 10 A 15 MINUTOS	Severo Bajo
DE 20 A 25 MINUTOS	Severo Medio
DE 25 EN ADELANTE	Severo Alto

Tabla 1. Matriz de identificación de vulnerabilidades de los sistemas de respuesta

Y una tabla que puede ser de utilidad para la programación de las pruebas de vulnerabilidad:

PLANIFICACIÓN PRUEBAS DE VULNERABILIDAD				
FECHA DE REALIZACIÓN:		RESPONSABLE DE PROGRAMAR LA PRUEBA:		
HORA DE REALIZACIÓN:		LUGAR EN EL QUE SE REALIZA LA PRUEBA:		
ESCENARIO	OBJETIVOS DE LA PRUEBA	EXPECTATIVAS	HALLAZGOS	RECOMENDACIONES

Tabla 2. Planeación de pruebas de vulnerabilidad

2. Modelo CPTED *(por su sigla en inglés: Crime Prevention Through Environmental Desing)* - "Prevención del crimen a través del diseño ambiental": el modelo consiste básicamente en invitar a delimitar los espacios públicos y privados de una forma adecuada, para poder identificar de manera clara las potenciales amenazas que existen en el entorno y que podrían ser generadoras de riesgos directos o indirectos. El diseño de la edificación debe ser pensado de tal forma que disuada la amenaza de cometer delitos dentro de los espacios controlados mediante los diferentes elementos de la seguridad (humana, electrónica) y el control del ambiente a través de diseños que permitan tener una adecuada visualización de la amenaza. La delimitación de los espacios es importante, ya que las personas deben "sentir" cuando salen o ingresan de un espacio privado a uno público, pues esto ayuda a generar sensación de seguridad, que contribuye a fortalecer la cultura de seguridad en el interior y exterior de las organizaciones.

Las instalaciones quedan resguardadas sin convertirse necesariamente en un fortín, que desde el punto de vista arquitectónico son agradables y generan confort en los usuarios y visitantes. El paisajismo, los amplios ventanales, la iluminación adecuada y permanente en espacios oscuros, el control total de los sitios de riesgo o áreas vulnerables, el control de acceso adecuado y suficiente, la seguridad humana, profesional y capacitada, y la señalización que indique a todas las personas que están siendo vigiladas y monitoreadas, son algunas de las variables que este modelo ofrece, y que en las instalaciones de nuestras organizaciones o compañías pueden ser de mucha utilidad para prevenir el crimen dentro y fuera, lo que reduce la probabilidad de ocurrencia y minimiza el impacto que esto pueda tener en las personas, sus pertenencias, así como en los activos de las compañías o en sus instalaciones. El modelo CPTED demuestra

que a través de tener un control adecuado, mantener limpios y aseados los predios y realizar mantenimiento a las instalaciones, se reducen los temas relacionados con vandalismo y oportunidad para cometer delitos.

De acuerdo con los diferentes estudios criminológicos realizados, la mayoría de los incidentes ocurren en lugares con poca o ninguna iluminación, la suciedad es permanente, no hay una delimitación adecuada entre lo público y lo privado, y no existen elementos de control que contribuyan con la disuasión.

Figura 1. Ejemplo de diseño ambiental CPTED

3. Modelo *JAMES REASON* o del queso suizo: si bien es cierto que es un modelo para la prevención de accidentes, se puede utilizar en el manejo y prevención de incidentes de seguridad, pues lo que sugiere este modelo es crear capacidad de seguridad que nos ayude a mitigar el impacto que un incidente de seguridad pueda tener en las personas, activos u operación.

Es un modelo fácil de implementar, y lo que muestra es que en la medida que mantengamos lo que queremos proteger alejado de la amenaza, se reduce la probabilidad de ocurrencia. La mayoría de las personas toleran el riesgo sin tener en cuenta el impacto, y lo que menciona este modelo es que el riesgo se puede controlar de una forma adecuada y eficaz, simplemente identificando las causas raíces y los factores de riesgo, para poder así determinar qué tipo de contramedida debemos utilizar; en el siguiente ejemplo podemos ver cómo lo podríamos implementar:

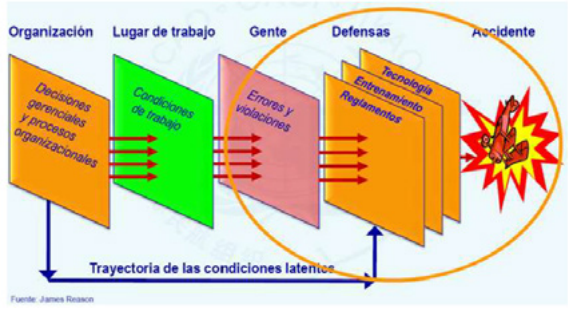


Figura 2. Ejemplo de diseño del modelo J. Reason

Se busca generar un sistema de "bloqueo o retardo", para que la amenaza tenga poca probabilidad de éxito en su actividad delictiva, ya que puede visualizar barreras en torno a lo protegido, que lo terminan disuadiendo y obligándolo a buscar un blanco más vulnerable.

4. Modelo de protección con profundidad: este modelo se utiliza originalmente por las áreas de seguridad de la información, se basa en llevar lo más valioso al centro de un esquema de seguridad rodeado de una serie de "círculos de protección", para reducir la probabilidad de éxito de la amenaza; este modelo centra su atención en todo lo relacionado con la información. Sin embargo, cuando lo revisamos de forma cuidadosa lo podemos emplear para proteger personas e instalaciones. Recuerden que lo fundamental es mantener lo más valioso o importante en el centro. El objetivo es generar disuasión, retardo y respuesta que la amenaza pueda percibir para que sienta la incertidumbre de que probablemente tendrá riesgos en el momento de su ingreso, pero también que podrá tener problemas en el momento de salir de las instalaciones o perímetro protegido.

Se busca con este modelo no solo generar disuasión, sino llegar a promover y mantener los factores de denegación, es decir, que el esquema de seguridad se perciba tan robusto y eficiente que la amenaza ni siquiera es capaz de probarlo, ya que no es fácilmente vulnerable.

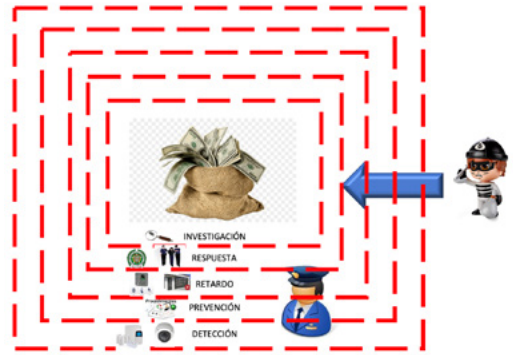


Figura 3. Ejemplo de modelo básico de protección con profundidad

Al implementar este modelo se reduce la probabilidad de ocurrencia cuando los sistemas de seguridad están acordes con el nivel de la amenaza. Sin embargo, si desean volverlo aún más robusto, deben tener en cuenta otras variables, como:

- Disuasión
- Denegación
- Recuperación
- Lección aprendida
- Pruebas de vulnerabilidad

Estos son los modelos que más se ajustan a nuestras operaciones de seguridad y que permiten dar un adecuado servicio de seguridad y protección a las grandes áreas de una compañía que requieren atención de seguridad:

a. Protección de personas
b. Seguridad de instalaciones
c. Seguridad en la cadena de suministro

Teniendo en cuenta lo anterior, podemos entonces hablar de la particularidad de crear un método que nos permita administrar la seguridad corporativa de una forma adecuada y efectiva, que busca reducir la probabilidad de ocurrencia de los incidentes de seguridad y que de ocurrir se logre mitigar el impacto para que los daños o las pérdidas puedan ser tolerables para cualquier organización.

En temas metodológicos, no existe un manual hecho en piedra que permita indicar que es sí, y solo sí, el único en el mercado, pues eso depende de los factores de riesgo directo o indirecto que tenga cada compañía o persona; sin embargo, es importante mencionar que para poder tener el mapa claro, es fundamental que se realice un análisis de riesgos teniendo en cuenta estas cuatro variables:

- Analizar el riesgo real de cada persona, operación o compañía.
- Identificar las amenazas del entorno (naturales, humanas, tecnológicas).
- Revisar las vulnerabilidades, para poder darnos cuenta de qué debemos hacer y cómo lo debemos hacer para mitigar el impacto y reducir la probabilidad de ocurrencia; los factores para tener en cuenta son: tiempo, frecuencia y exposición.
- Determinar el impacto para poder establecer la potencialidad en términos de daños y pérdidas.

Luego de esto, es importante revisar los aspectos tácticos del esquema, y esto está relacionado con lo que vamos a utilizar en cuanto a contramedidas de seguridad; en la siguiente figura podrán tener un claro ejemplo de estas contramedidas:

- *Esquema táctico de seguridad:*

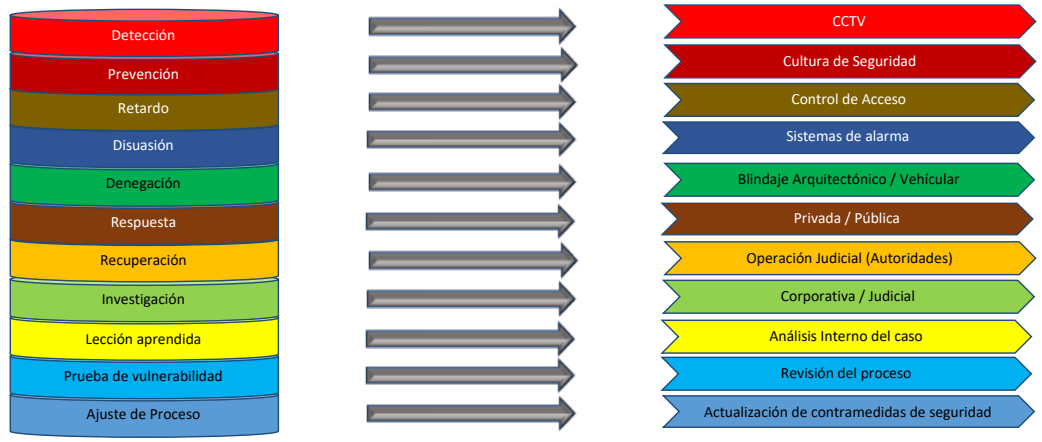


Figura 4. Esquema táctico de protección

Teniendo en cuenta lo anterior, ahora debemos pensar en cómo integramos todo esto en un método de seguridad efectivo y eficaz, que nos permita presentar a la alta gerencia un sistema integrado de gestión de seguridad que ayude al negocio a funcionar con un nivel tolerable de riesgos y que mantenga los impactos en un rango aceptable. Para ello hemos diseñado y proponemos lo siguiente:

Figura 5. Esquema estratégico de protección

Esta breve explicación pretende que aquellas personas que se interesan por conocer lo metodológico de la seguridad puedan implementar esquemas de seguridad y protección lógicas y adecuadas, teniendo en cuenta que se parte de las bases teóricas, operativas, tácticas y estratégicas. Los profesionales de seguridad en muchos casos pasamos por alto la importancia de partir de la base de modelos de seguridad que nos pueden ayudar a administrar mejor el riesgo, fortaleciendo nuestros recursos en cuanto a mitigar los riesgos y reducir los impactos de los incidentes que puedan suceder. Por ello es necesario tener en cuenta que la herramienta más importante es la de fortalecer los mecanismos y aptitudes de detección tanto en el ámbito humano como en el electrónico. Nada puede ser dejado al azar, y por eso una vez que se implementen o instalen las contramedidas de seguridad, se sugiere realizar las pruebas de vulnerabilidad para determinar si esa contramedida está siendo efectiva en términos de detección, prevención, retardo, disuasión y respuesta.

CAPÍTULO 3

LA OCDE Y EL SECTOR EMPRESARIAL EN COLOMBIA: RETOS Y TRANSFORMACIONES ANTE EL COMERCIO INTERNACIONAL

3. La OCDE y el sector empresarial en Colombia: Retos y transformaciones ante el comercio internacional

Por: Teniente Coronel (RA) Jesús Eduardo Moreno Peláez
Auditor Internacional BASC

Resumen

En este capítulo se analizarán los retos que enfrentan las empresas colombianas en los mercados internacionales, donde la cooperación se ha convertido en una herramienta para poder competir. En el caso colombiano, se logró la integración dentro de la Organización para la Cooperación y el Desarrollo Económico (OCDE), por lo cual se debe pensar en una política pública que concrete el aprovechamiento de esta nueva oportunidad ante el comercio internacional. Tarea que no es exclusiva del Estado, sino que debe estar fomentada y apoyada por el sector empresarial. Así, resulta relevante determinar qué mecanismos permiten este aprovechamiento, y la herramienta idónea es el Sistema de Control y Gestión del Riesgo BASC y la Norma y Estándares Internacionales Versión 5 - 2017.

Palabras clave

OCDE, comercio internacional, cadena de suministros, BASC.

Introducción

Dentro de un mundo cada vez más globalizado, la interacción entre empresas rompe con cualquier frontera, gracias al libre comercio y los avances de la tecnología, lo que representa un gran reto para las empresas, pues deben cambiar y mejorar sus modelos tradicionales de producción y comercialización (Valencia & Ortiz, 2017, p. 57) para responder a este escenario, en el que la competitividad se vuelve el factor medida para el desarrollo. De este modo, las empresas deben establecer las herramientas más adecuadas que les permitan tener una participación reconocible dentro de dichos mercados, como lo es la cooperación internacional.

En el caso de Colombia, esta cooperación se ha materializado con su integración en la OCDE, presentándose como cuestionamiento ante la competitividad del comercio internacional, la forma mediante la cual el sector empresarial de Colombia puede cumplir con los estándares de este organismo y, con ello, mejorar su competitividad con apoyo del Estado.

La respuesta ante esta pregunta es el fin de este capítulo, para lo cual se analizarán los siguientes elementos, que puedan llegar a una propuesta de solución: primero, la importancia de la cadena de suministros (en adelante CSu) dentro del comercio internacional; posteriormente, las políticas o estándares propuestos por la OCDE en materia de la CSu, y por último, las herramientas idóneas que permitan a las empresas cumplir con estos estándares, como lo son la Norma y Estándares Internacionales BASC, que se consolidan como el conjunto de normas que permiten establecer y evaluar el Sistema de Control y Seguridad dentro de la CSu.

1. El papel de la cadena de suministros dentro del comercio internacional

Para iniciar, se presentará el concepto de comercio internacional, entendido como "el intercambio de bienes y servicios que realiza la economía de un país o área regional con las economías de otros países o áreas regionales" (Cervera, 2011, p. 5), intercambios que se han transformado en la actualidad. El siguiente mapamundi demuestra el contexto en el que se encuentra Colombia:

Mapa 1. PIB por regiones, estimación 2019

Fuente: Indicadores económicos FMI (2018)

Colombia se encuentra en un escenario económico donde Estados Unidos, con la política "America First", ha dejado varios de los mercados abiertos. Además, el crecimiento de China, junto con las diferentes economías emergentes que han surgido por todo el mundo, es muestra de la existencia de un escenario económico de alta competitividad. No obstante, para el caso colombiano resulta favorable tener una proyección de crecimiento en la región, que permita su inclusión en un nuevo mercado, como se demuestra en la siguiente gráfica:

Gráfica 1. Crecimiento del PIB 2016-2019

Fuente: Indicadores económicos FMI (2018)

Este panorama evidencia nuevas oportunidades, que se pueden aprovechar con mercados en los cuales es posible que participen las empresas colombianas, al asumir la competitividad intrínseca a este contexto, que puede ser afrontado gracias a la cooperación internacional a través de la OCDE; sin embargo, para poder optar por los beneficios de esta organización, Colombia debe asumir transformaciones del sector público, además del fomento y apoyo del sector.

Para lograr lo anterior, se debe establecer cuál de las etapas dentro del comercio internacional pueden ser mejoradas, y de esta manera asumir capacidades para aprovechar positivamente los diferentes mercados en los cuales, gracias a la cooperación internacional, puede ingresar Colombia y su sector empresarial. La etapa que debe ser objeto de transformación es aquella que tenga mayor incidencia dentro del intercambio de bienes y servicios, y en este caso es la CSu, dado que cubre los diferentes procesos que integran el intercambio desde la materia prima hasta el producto final, que es llevado al consumidor. Se refuerza la importancia de esta etapa en el comercio internacional, debido a que

> "abarca todas las actividades asociadas con el flujo y transformación de bienes e información asociada desde la fase de materias primas hasta el usuario final. Es esencialmente un conjunto de proveedores y clientes conectados; donde cada cliente es a su vez proveedor de la siguiente organización 'aguas abajo' hasta que el producto terminado alcanza al usuario final" (Vilana, 2010, p. 6).

De esta manera, la CSu no se aísla a procesos netamente internos dentro de la empresa, sino que reconoce las dinámicas externas, teniendo una inmersión total dentro del intercambio de bienes, y en algunos casos también de servicios del comercio internacional. Esta CSu dentro del comercio internacional adquiere mayor valor al ser una parte fundamental de las cadenas de valor, debido a que es un producto de la reducción de los costos de transporte y la revolución de la tecnología de la información, cuyos avances han brindado a las

empresas la capacidad de coordinar sus necesidades de producción en tiempo real, sin importar la ubicación geográfica del productor (Stephenson, 2014, p. 1)[1].

Mediante la siguiente gráfica, de forma simplificada se evidencia la prevalencia de la CSu dentro de los procesos de intercambio del comercio internacional, pues entre cada uno de los actores y empresas que puedan interactuar en determinado proceso, existen fases de transporte que son parte de la CSu, sin olvidar que mediante el Sistema de Control y Seguridad sobre la CSu vincula entre estos a actores, por la existencia de relaciones de proveedor y consumidor.

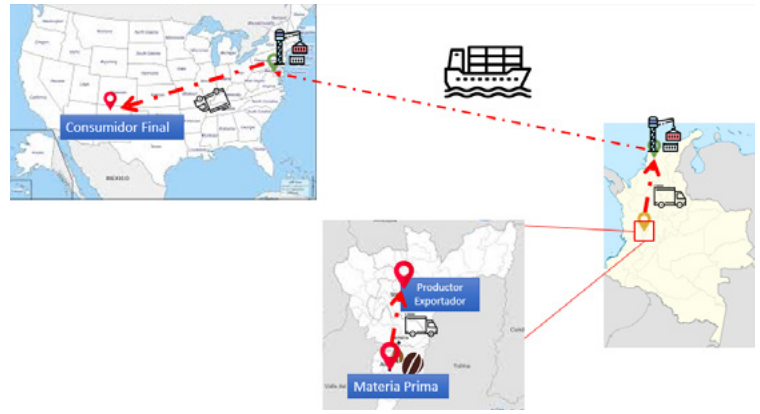


Ilustración 1. CSu y comercio internacional

Fuente: Elaboración propia

En el ejemplo que se describe en la ilustración anterior se demuestra la existencia de cadenas entre los actores nacionales e internacionales, que interactúan entre sí para lograr llevar el producto final al consumidor, sin distinción de las fronteras terrestres o marítimas que ello implique, quedando claro que entre estos actores existen relaciones de proveedor y consumidor, integrando aún más la CSu. Con todo lo anterior, se evidencia que la CSu se consolida como la etapa prevalente dentro del comercio internacional.

2. Estándares OCDE en materia de CSu

Una vez sustentada la importancia de la CSu como una parte principal dentro del comercio internacional y, por ende, el foco para la gestión de las transformaciones del sector empresarial, con el fin de mejorar las capacidades para entrar en los nuevos escenarios de competitividad dentro del mercado internacional, es importante recalcar la incidencia que tiene para Colombia

1 Este mismo autor hace relevancia a que las autoridades competentes tengan en consideración una adecuada política pública respecto de la cadena de suministros y su prevalencia dentro del comercio internacional, al integrarse dentro de la cadena de valor, pues él manifiesta que los legisladores (autoridades públicas), para la construcción de políticas comerciales (Stephenson, 2015, p. 1), deben tener claridad sobre esta cadena.

poder, mediante la cooperación internacional por medio de la OCDE, mejorar estas capacidades, pero especialmente lograr obtener los beneficios que este tipo de vínculo genera al abrir nuevas oportunidades de desarrollo, en el que puede participar Colombia. De esta manera, las condiciones de calidad en la CSu, que deben ser cumplidas por parte no solo del Estado colombiano, sino también de las empresas, son estándares que ya ha categorizado la OCDE. Esta corporación ha postulado documentos de los años 2017 y 2018 que tratan el tema de la cadena de suministro; los criterios que son expuestos en el documento "Building Supply Chain Resilience: A Review of Challenges and Strategie" son:

i) Fomentar una cultura de gestión de riesgos (OECD, 2014, p. 13); ii) mitigar el riesgo dentro de los sistemas internos de producción y logística (OECD, 2014, p. 13); iii) fortalecer las acciones riesgosas de colaboración en la cadena de suministro (OECD, 2014, p. 14); iv) compartir información de riesgo con socios de la cadena de suministro; v) aumentar la agilidad de la cadena de suministro; vi) aumentar la redundancia/inventario en puntos críticos; vii) supervisar y analizar las faltas cercanas; viii) sistemas de prueba de estrés regularmente.

Cada uno de los criterios antes descritos se convierten en elementos que deben estar insertados en la política pública que fomente el desarrollo económico del país, pues, como se ha consolidado en los numerales anteriores, la CSu resulta ser una etapa en la cual se determina el éxito de los diferentes intercambios comerciales; en este sentido, es un elemento y actividad que generan un alto interés por parte de las diferentes autoridades competentes, apoyando el cumplimiento de los criterios anteriormente descritos por cada una de las empresas, logrando de esta manera llegar a los estándares de calidad OCDE y poder disfrutar los beneficios que se obtienen con ello.

3. Pertinencia de BASC en relación con el Sistema de Control y Seguridad en la cadena de suministros

Dentro de los focos que deben tenerse en cuenta para la transformación del sector empresarial de cara al comercio internacional, se debe determinar aquella etapa que abarque el mayor porcentaje respecto de la totalidad del proceso vinculado al intercambio, como lo es la CSu, según ya se ha tratado, etapa sobre la cual la OCDE ya se ha pronunciado y estipulado parámetros que deben ser cumplidos por las empresas con el apoyo del Estado, quedando como cuestionamiento la herramienta que puede ser implementada con el objeto de alcanzar estos estándares.

El objetivo es mejorar las condiciones y capacidades del sector empresarial en materia de CSu, al generar con ello un mayor impacto sobre las capacidades que pueden obtener las empresas con relación a los retos competitivos que se generan dentro de los mercados internacionales, más aún teniendo en consideración la necesidad de alinear esta transformación respecto de los criterios postulados por la OCDE, objetivos que se pueden alcanzar a través de la implementación de la Norma y Estándares Internacionales BASC, pues se consolidan como un conjunto de normas que surgen del propio sector

empresarial con apoyo de entidades públicas, para consolidar el Sistema de Control y Seguridad en la CSu, siendo pertinentes para lograr las transformaciones que se han venido manifestando a lo largo de este documento, con el fin de mejorar las capacidades que permitan asumir los retos igualmente descritos sobre el mercado internacional.

En este orden de ideas, es oportuno presentar la definición sobre la Norma y Estándares Internacionales BASC, los cuales son estatutos establecidos para promover el comercio internacional seguro creado entre las empresas del sector privado y organismos nacionales y extranjeros, cuyo objetivo principal es la lucha contra el narcotráfico y la contaminación de la carga en la cadena logística. BASC proyecta unos beneficios que pueden adquirir tanto empresas como gobiernos y aduanas, influyendo y apoyando la relación que se da entre lo público y lo privado, con el fin de evitar los delitos y suministrar mayor confianza y colaboración entre los dos sectores.

Sobre la cadena de suministros, BASC ha proferido la norma internacional BASC: Sistema de Gestión en Control y Seguridad Versión 5, del 2017, la cual tiene por objeto,

> "a) Establecer, documentar, implementar, mantener y mejorar el Sistema de Gestión en Control y Seguridad. b) Asegurar el cumplimiento de los compromisos establecidos en la política de gestión en control y seguridad. c) Gestionar los riesgos con base en el enfoque en procesos. d) Demostrar su capacidad para mantener la integridad de la cadena de suministro. e) Implementar y mantener programas tales como C-TPAT y Operador Económico Autorizado, OEA y otros" (BASC, 2017, p. 4).

Con lo anterior se demuestra la pertinencia de esta normatividad para lograr mejorar las capacidades de las empresas en relación con la CSu, pues con el Sistema de Gestión en Control y Seguridad (SGCS BASC) se logra integrar dentro de las empresas una visión contextual y global que permite optar por una decimada inserción dentro del mercado internacional. De esta manera, el SGCS BASC postula como presupuesto para la certificación en la CSu los componentes que se describen a continuación.

Contexto de la empresa, en el que las empresas deben tener una comprensión de la corporación y de su contexto, además de la comprensión de las necesidades y expectativas de las partes interesadas, lo que implica establecer el alcance del SGCS BASC, además de los enfoques en procesos (BASC, 2017, p. 4); asimismo, la empresa debe establecer un componente de liderazgo por parte de la alta dirección, lo que implica que la compañía estipule la política de gestión en control y seguridad, objetivos del SGCS BASC, y la responsabilidad y autoridad en la empresa (BASC, 2017, p. 9); otros de los componentes son la planificación, gestión de riesgos, requisitos legales, apoyo, recursos, información documentada, evaluación del desempeño, seguimiento, medición, análisis y evaluación, auditoría interna, mejoras. Cada uno de estos elementos, que integra el SGCS BASC, responde a la demanda exigida por parte de la OCDE,

comprobándose de esta manera en referencia a la CSu como etapa de alto impacto dentro del comercio internacional, siendo la herramienta principal para que las empresas, con el apoyo del Estado, puedan generar transformaciones de cara a la competitividad que generan los mercados internacionales. Más aún si se considera que "contar con un SGCS BASC le permitirá a la empresa organizar sus procesos internos, contar con una política organizacional, visión, misión y objetivos, los cuales deben ir acorde al plan estratégico que la empresa desarrolle con la finalidad de cumplir con las metas trazadas para un periodo determinado" (Aguayo & Valverde, 2016).

Conclusiones

Con todo lo descrito en este documento, se evidencia la importancia de la cadena de suministro para el mercado internacional de las empresas colombianas, pues este escenario es muy competitivo, ante lo cual la cooperación internacional permite beneficios para ingresar a nuevos mercados o mejorar las capacidades en los que ya participan, pero para ello necesitan cumplir con estándares de calidad, siendo importante apoyarse en la Norma y Estándares Internacionales BASC, que se adecúan a los parámetros OCDE y consolidan el Sistema de Gestión en Control y Seguridad en la cadena de suministros.

Referencias

Aguayo Campoverde, D. A. & Valverde Maldonado, M. D. (2016). *Sistema de Gestión en Control y Seguridad (SGCS) BASC, como herramienta de marketing internacional para los agroexportadores peruanos.* Perú: Escuela Profesional de Administración de Negocios Internacionales.

BASC (2017). Norma Internacional BASC: Sistema de gestión en control y seguridad. World BASC Organization.

Cervera, D. R. (2011). *Métodos y técnicas de investigación internacional.* España: Universidad Complutense de Madrid.

OECD (2013). *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas (Second Edition).* Paris: OECD Publishing.

OECD (2014). *BUILDING SUPPLY CHAIN RESILIENCE: A Review of Challenges and Strategies.* Paris: OECD Publishing.

OCDE (2016). Principios de Gobierno Corporativo de la OCDE y del G20. Paris: Éditions OCDE. http://dx.doi.org/10.1787/9789264259171-es

OCDE (2017). Recomendación del Consejo de la OCDE sobre integridad pública. Paris: Éditions OCDE. http://www.oecd.org/gov/integridad/recomendacion-integridad-publica/

Stephenson, S. (2014). *Global value chains: the new reality of international trade. By International Centre for Trade and Sustainable Development* (ICTSD), 7 Chemin de Balexert, 1219 Geneva, Switzerland.

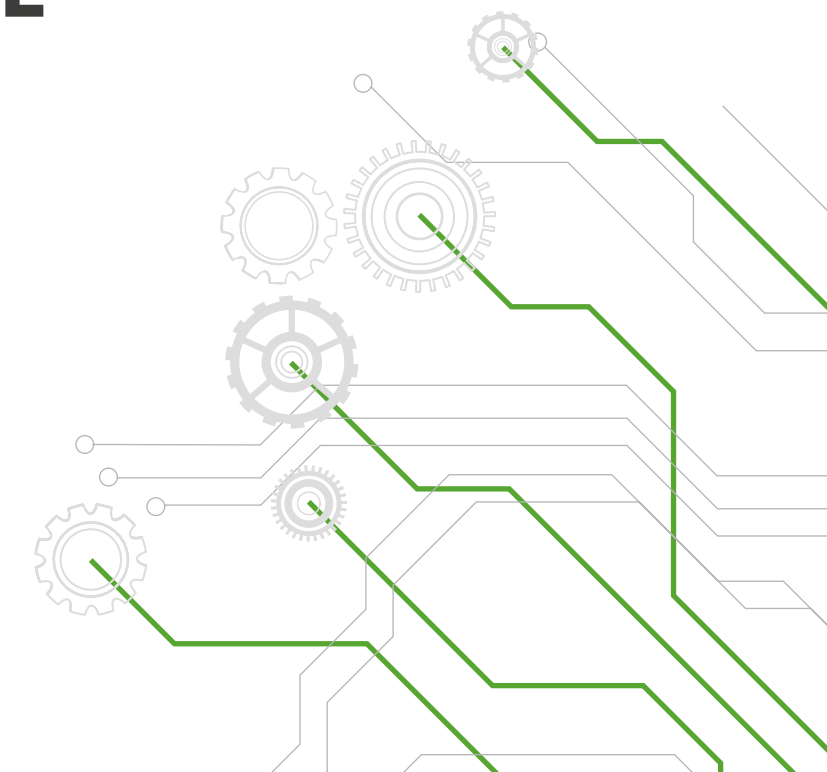
Stephenson, S. M. (2015). *Cadenas globales de valor: la nueva realidad del comercio internacional* (pp. 23-57). International Centre for Trade and Sustainable Development.

Valencia, J. B. & Ortiz, E. P. G. (2017). Competitividad y comercio internacional. *Revista de Investigación en Ciencias de la Administración, 9* (16): 49-58.

Vilana, J. R. (2010). *La gestión de la cadena de suministro.* Escuela de Organización Industrial.

CAPÍTULO 4

EL FRAUDE: UN FLAGELO QUE IMPACTA A LAS EMPRESAS A NIVEL MUNDIAL



4. El fraude: un flagelo que impacta a las empresas a nivel mundial

Por: Instituto Nacional de Investigación y Prevención de Fraude - INIF

Marco normativo
Constitución Política de Colombia 1991
Artículo 83. Las actuaciones de los particulares y de las autoridades públicas deberán ceñirse a los postulados de la buena fe, la cual se presumirá en todas las gestiones que aquellos adelanten ante estas.
Código Penal Colombiano: Ley 599 del 2000
Artículo 246. Estafa. **Artículo 323.** Lavado de activos. **Artículo 103.** Homicidio. **Artículo 435.** Falsa denuncia. **Artículo 442.** Falso testimonio. **Artículo 322.** Favorecimiento por servidor público. **Artículo 453.** Fraude procesal. **Artículo 340.** Concierto para delinquir. **Artículo 289.** Falsedad en documento privado. **Artículo 287.** Falsedad en documento público. **Artículo 286.** Falsedad ideológica en documento público.
Código de Comercio: Decreto 410 de 1971
Artículo 1058. Declarar sinceramente todas las circunstancias inherentes al riesgo. **Artículo 1060.** Mantener el estado de riesgo. **Artículo 1061.** Cumplir estrictamente con las garantías. **Artículo 1066.** Pago efectivo de la prima. **Artículo 1093.** Informar la contratación de otros seguros respecto del mismo objeto asegurado. La no observancia de esta obligación producirá la terminación del contrato. **Artículo 1103.** No asegurar la parte dejada en descubierto, cuando se pacta coaseguro obligatorio. **Artículo 981.** Contrato de transporte **Artículo 982.** Obligaciones del transportador, numeral 1. **Artículo 986.** Regulación de la responsabilidad cuando intervienen varios transportadores. **Artículo 987.** Transporte multimodal.

El fraude es una conducta que genera preocupación en las empresas alrededor del mundo, por su impacto y las consecuencias que tiene en los activos económicos y reputacionales. En la 15.ª Encuesta Global de 2018, sobre integridad en los negocios, se expresa que el fraude y la corrupción son los principales riesgos corporativos que van en aumento (Ernst & Young, EY, 2018).

De acuerdo con la Association of Certified Fraud Examiners (ACFE), el fraude "incluye cualquier acto intencional o deliberado de privar a otro de una propiedad o dinero, por la astucia, el engaño u otros actos desleales"; así mismo, apoyada en la definición de Black's Law Dictionary, la ACFE describe este flagelo como "una declaración falsa a sabiendas de la verdad o la ocultación de un hecho material para inducir a otro a actuar en su detrimento". Según Price Benowitz LLP (2017), "el daño o perjuicio que resulta de esta práctica deshonesta es típicamente un daño económico", y se describe como "un acto intencionado realizado por una o más personas de la dirección, los responsables del gobierno de la entidad, los empleados o terceros, que conlleva la utilización del engaño con el fin de conseguir una ventaja injusta o ilegal" (NIA-ES 240, 2013), por lo que la razón principal detrás de la acción fraudulenta es alcanzar una ganancia por medio de términos ilegales (Alexopoulos, Kafentzis, Benetou, Tagaris & Georgolios, 2007).

A partir de lo anterior, se identifican cuatro elementos que caracterizan todo acto fraudulento: a) se trata de un acto clandestino; b) se hace uso de las funciones de la organización; c) se comete para obtener ganancias monetarias, y d) impacta en los activos o ganancias de la empresa (Saksena, 2012, citado en Borda, 2015).

Por su parte, el Instituto Nacional de Investigación y Prevención de Fraude (INIF) clasifica este flagelo, según el rol del defraudador, en: **fraude interno,** en donde un empleado de la compañía es quien comete la acción; **fraude externo,** el cual es llevado a cabo por una persona ajena a la misma, y **fraude mixto,** que involucra la participación de un colaborador en alianza con un externo; en cualquiera de estos casos se busca obtener un beneficio o provecho a través del engaño (INIF, 2018a).

Así mismo, la teoría del Triángulo del Fraude propone que la comisión de este flagelo involucra la presencia de un problema (presión) que no se puede compartir, esto es, una dificultad que en secreto podría resolverse mediante el abuso de la confianza otorgada a la persona según su contexto (Rodríguez & Gartner, 2017); además, debe haber una oportunidad para abusar de la confianza y consumar el acto fraudulento; este elemento involucra la percepción de entornos vulnerables y escenarios que ofrecen "un potencial atractivo de recompensa criminal con poco riesgo aparente de detección o penalización" (Ramamoorti, 2008, p. 524). Una vez que lo realiza la persona, genera racionalizaciones o justificaciones que hacen ver su comportamiento como algo apropiado; otra forma de entenderlo es como una serie de verbalizaciones que elabora el defraudador, con el fin de "mantener su imagen de no culpable o no responsable de la situación fraudulenta" (Galvis & Santos-Mera, 2017, p. 76).

Así, estos criterios conforman los tres componentes que actualmente integran el modelo clásico: (1) presión, (2) oportunidad y (3) racionalización (ver figura 1). Según Cressey (1953, citado en Lokanan, 2015), los elementos deben aparecer en este orden preciso para que el fraude sea consumado.

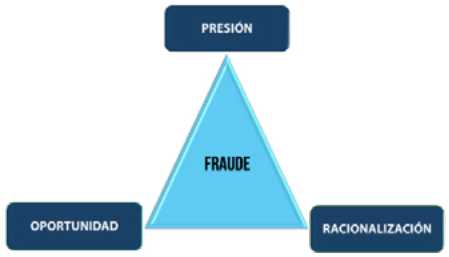


Figura 1. Elaboración propia, basada en el Triángulo del Fraude de Cressey (1953).

Posteriormente, Wolfe y Hermanson (2004) propusieron la integración de un cuarto elemento: la capacidad, que se entiende como habilidades personales que desempeñan un papel importante para la comisión del fraude (ver figura 2).

Figura 2. Elaboración propia, basada en el Diamante del Fraude de Wolfe y Hermanson (2004).

La capacidad consta de seis componentes. En primer lugar, se encuentra el cargo que se ocupa en la empresa, donde a mayor rango corporativo, mayor propensión a cometer fraude. El segundo es la habilidad de explotar o crear oportunidades, aprovechándose de las debilidades de la empresa en cuanto a accesos e información (Beasley *et al.*, 1999, citado en Wolfe y Hermanson, 2004; Schuchter & Levi, 2015; Dellaportas, 2013; López & Sánchez, 2012).

El tercero se refiere a la gran confianza que tiene el defraudador en no ser descubierto. El cuarto corresponde a las habilidades para coaccionar a una persona; es decir, el uso de la persuasión para convencer a otros en una situación de fraude (Allan, 2003, citado en Wolfe y Hermanson, 2004).

El número cinco es la capacidad que tiene el defraudador para ser convincente

y mantener la mentira, de tal forma que sea coherente y constante. El último es la inmunidad al estrés (Wolfe y Hermanson, 2004).

Lo anterior es evidencia de que el fenómeno del fraude es un comportamiento complejo, enmarcado en un contexto social, empresarial y normativo que implica un estudio interdisciplinario para entenderlo y atacarlo de manera efectiva. Además, y dadas sus implicaciones, se ha convertido en un problema potencial para la economía mundial, como se evidencia a continuación:

Panorama nacional e internacional del fraude

El fraude se fortalece con el paso del tiempo, pues de acuerdo con PricewaterhouseCoopers (PwC), el 49% de los encuestados indicaron que su compañía ha sido víctima de este en los últimos dos años, lo cual representa un aumento del 36% en comparación con el 2016 (PwC, 2018a).

Dentro de las consecuencias que ha dejado este flagelo, se encuentra que en el 45% de los casos se reportaron pérdidas económicas hasta de 100 mil dólares a nivel global, y en el 30% hasta de 5 millones de dólares en daños (PwC, 2018b) (figura 3).

Figura 3. Pérdidas económicas a causa del fraude. Elaboración propia, basada en PwC (2018b).

Además del costo económico, el fraude influye en la confianza que tienen los grupos de interés en la marca, y se afectan así las relaciones comerciales entre ellos (PwC, 2018a).

Para el caso de Latinoamérica, el fraude alcanzó un 53%, y mostró un aumento del 25% entre el 2016 y el 2018 (PwC, 2018a). En la 15.ª encuesta global sobre integridad en los negocios (EY, 2018), se reporta que el 14% de las empresas en Sudamérica han sufrido fraudes significativos en los últimos dos años, y el 74% percibe que este flagelo se está fortaleciendo.

En Brasil se identificó que el 54% de las empresas fueron defraudadas, y según la percepción del 29% de los empresarios, existe una alta vulnerabilidad para que este se cometa (Kroll, 2012); adicionalmente, en el 2018 el 96% de los brasileños reconoce el soborno y la corrupción como prácticas habituales en sus organizaciones. En otros países, como México, se ven seriamente afectados, pues aumentó el número de compañías que reportaron incidentes de fraude, al pasar de un 37% en el 2016 a un 58% en el 2018 (PwC, 2018e).

Desde la perspectiva nacional, durante el 2017 más de la mitad de las organizaciones colombianas experimentaron algún tipo de fraude, que representó una pérdida económica cercana a los 10.000 dólares, según lo

expresaron el 45% de los empresarios que participaron en la Encuesta de Fraude en Colombia (KPMG, 2017).

El 33% de los encuestados reportó fraude externo, y el 63%, interno; así mismo, se presentaron cinco principales modalidades: fraude al consumidor (19%), malversación de activos (58%), soborno y corrupción (31%), cibercrimen (27%) y mala conducta comercial (19%) (PwC, 2018d).

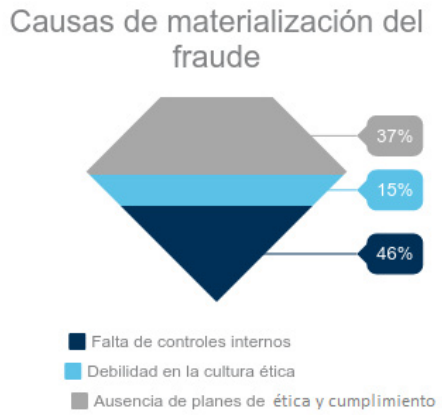


Figura 4. Causas que permiten la materialización de fraude en las empresas. Elaboración propia. basada en PwC (2018d).

Algunas de las causas que permitieron que el fraude se materializara fueron la falta de controles internos (46%), la debilidad en la cultura ética (15%) y el bajo índice de planes de ética y cumplimiento (37%) (KPMG, 2017) (figura 4). De igual forma, solo el 16% de los encuestados señalan haber realizado valoraciones de riesgo relacionadas con lavado de activos, sanciones y control de exportaciones, y apenas el 50% afirman que ejecutan evaluaciones de riesgo (PwC, 2018d).

Las variables organizacionales antes mencionadas propician el escenario ideal y hacen a la compañía vulnerable para la comisión de este flagelo.

Borda (2015) describe algunas de las principales oportunidades que se pueden presentar en un entorno financiero:

- Ausencia o falencias en los controles
- Debilidades en la supervisión
- Ausencia o debilidades en los programas antifraude, políticas y/o procedimientos
- Falta de medidas de aprehensión o estructuras organizativas
- Debilidades en la formación de los empleados
- Ausencia de segregación de funciones
- Debilidades del Comité de Auditoría y/o de la Junta Directiva
- Falta de supervisión y control externo

Vale la pena mencionar que una de las industrias más afectadas por el fraude es la aseguradora, pues, de acuerdo con el 37% de los encuestados, el sector es altamente vulnerable a la delincuencia económica (PwC, 2016), además de que ocupa el sexto lugar que más pérdidas genera por casos de soborno y corrupción (KPMG, 2018) (figura 5).

Considerando lo anterior, es importante darle una mirada más profunda al fraude en los seguros, para conocer el impacto que tiene en este contexto.

Figura 5. Sectores en donde el fraude ha tenido mayor impacto. Elaboración propia, basada en KPMG (2018).

El fraude en el sector asegurador

Considerando la alta propensión que tiene la industria aseguradora de sufrir incidentes de fraude, se han realizado diversas aproximaciones al concepto de fraude a los seguros. Mercedes Ayuso, miembro del equipo de investigación en riesgos en finanzas y seguros de la Universidad de Barcelona (España), lo define como aquella situación en "donde el asegurado pretende obtener un beneficio ilícito de la entidad aseguradora", que normalmente no puede contratarse, pagar una prima más baja o reclamar el pago de una indemnización, que por su motivo o cuantía no es justificada (1998, p. 6).

En contraste, la Coalition Against Insurance Fraud afirma que "el fraude de seguros ocurre cuando la gente engaña a la compañía o agente de seguro para cobrar dinero al cual no tiene derecho. De la misma forma, aseguradoras y agentes también pueden defraudarse entre sí o al consumidor".

Woolley y Gill (1994, citados en De la Espriella, 2012) definen este fraude como "la realización intencional de una reclamación ficticia, que busca inflar el valor o agregar costos extras o actuar deshonestamente con la intención de obtener más de lo legítimamente estipulado" (p. 565), mientras que INIF lo conceptualiza como "todo acto u omisión tendiente a obtener ilegalmente un beneficio proveniente de un contrato de seguros" (2007, p. 7).

Para conocer sobre la dinámica de fraude a los seguros es importante analizar su modus operandi, en el que se encuentran el fraude duro y el blando. INIF (2015), basándose en la definición de la Coalition Against Insurance Fraud, indica que el primero es la simulación **intencional** de una lesión, accidente, robo, incendio u otra pérdida para cobrar ilegalmente un dinero a la compañía de seguros; de igual forma, este tipo de fraude tiende a ser **recurrente** y **planeado** por bandas criminales.

Por su parte, el fraude blando se presenta cuando las personas honestas se aprovechan del siniestro para aumentar su reclamación; este es **ocasional** y **oportunista,** lo que hace que su detección sea más difícil (INIF, 2015).

Para detectar de este flagelo también se deben revisar los indicadores de fraude, que hacen referencia a "conductas particulares, señales de alerta o situaciones atípicas, que al ser descubiertas en una operación (suscripción, modificación, renovación, siniestros…) requieren de un especial seguimiento e investigación" (INIF, 2007, p. 7).

Para dimensionar la gravedad de este flagelo, vale la pena resaltar algunas cifras que muestran la evolución y el panorama general de su impacto. Específicamente para el caso de Colombia, en el 2012, según los casos analizados por INIF (citado por De la Espriella, 2012), se estimó que el fraude en seguros superó los 5.000 millones de pesos en el país; en ese año, el fraude en seguros de vida fue el más frecuente.

Además, alrededor del 10% de las reclamaciones se consideraban fraudulentas, donde el SOAT (Seguro Obligatorio de Accidentes de Tránsito) se destacó por ser uno de los productos mayoritariamente afectados, con cifras entre el 7 y el 9%, lo que representó en el 2015 un costo económico de 100.000 millones de pesos en fraude (Federación de Aseguradores Colombianos - Fasecolda, 2016).

Las repercusiones no solo se traducen en altos costos monetarios para la industria, sino también en pérdidas de ahorro, incremento de primas de seguros, desconfianza en el sector y, por ende, en desprotección de la sociedad (De la Espriella, 2012).

Lina María Chacón, gerente de INIF, en marzo del 2016 señaló que el nivel de fraude que hay en la industria aseguradora colombiana alcanzó el 7% del valor de las reclamaciones, y afirmó que:

El fraude va en aumento y abarca las pólizas de vida, salud, hogar y productos ligados a los servicios públicos, en los que el nivel de fraude es importante porque se paga una prima muy baja (unos 5.000 pesos mensuales), en tanto que la cobertura puede alcanzar hasta los 2 o 3 millones de pesos (citado en Fasecolda, 2016).

Durante el 2018, de acuerdo con los casos investigados por INIF, en el 18,4%[1] de las compañías del sector asegurador se determinó que el índice de fraude

[1] Porcentaje de participación de las compañías, con base en las primas emitidas netas de compensación reportadas en las estadísticas del sector ofrecidas por Fasecolda (2018).

fue del 9%, representado en un ahorro de 10.073.222.097 pesos, lo cual implica que de no haber identificado estas conductas a tiempo, las compañías habrían pagado reclamaciones ilegítimas que al final se verían reflejadas en pérdidas millonarias en sus estados financieros. A continuación (figura 6) se representa la tasa de detección de fraude en las compañías, y se evidencia que los picos más altos se encuentran entre septiembre y octubre, con una tasa del 10,5%, cifra que se encuentra por encima del índice reportado en el 2017, que era de 8,5% (INIF, 2017).

Detección de fraude en el sector asegurador, 2018:

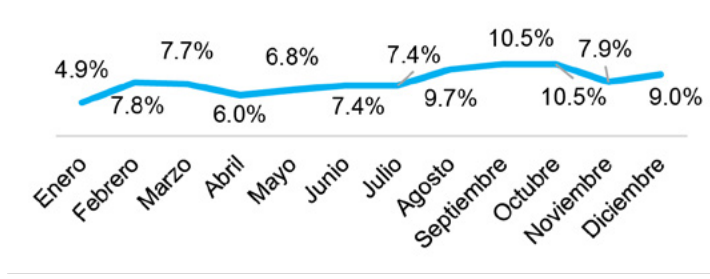


Figura 6. Detección de fraude en los casos investigados por INIF en el 18,4% del sector asegurador mes a mes (2018b).

Lo anterior indica que la gestión de INIF en términos de investigación y detección de fraude ha sido efectiva; no obstante, es de vital importancia fortalecer los mecanismos actuales, con el objeto de aumentar la tasa de detección y formular estrategias preventivas y correctivas para combatir efectivamente el fraude.

Vale la pena resaltar que el fraude impacta directamente la operación del sector asegurador. De acuerdo con el Boletín de Estadísticas No. 008 (2019) de Fasecolda, la operación técnica de la industria de seguros evidenció una pérdida de 1,8 billones de pesos para el año 2018, una cifra que podría disminuir mediante acciones de detección y prevención efectivas de fraude (Nájera, 2019).

Sin embargo, a pesar del evidente daño que genera esta conducta, el fraude no está tipificado como un delito en el código penal colombiano, lo cual hace que el principal foco de interés sean los delitos de "mayor impacto social", como lo son hurto, homicidio, violaciones, violencia intrafamiliar, etc., restándole importancia a las consecuencias sociales, judiciales y económicas que este tiene (Fernández, Niño y Cabrera, 2005).

Con base en lo anterior, INIF logró, dentro de la legislación penal colombiana, que la conducta de fraude a los seguros específicamente esté catalogada como un agravante del delito de estafa (artículo 246), y puede relacionarse con otros, como: lavado de activos (artículo 323), falsedad en documento (capítulo III), homicidio (artículo 103), falsa denuncia (artículo 435), falso testimonio (artículo

442), favorecimiento (artículo 322), fraude procesal (artículo 453) y concierto para delinquir (artículo 340), según las características del hecho, el modus operandi del defraudador y los medios utilizados para su ejecución (Código Penal Colombiano, 2000).

Adicionalmente, según lo mencionado por Vásquez (2017), los contratos de seguros están amparados por el principio de buena fe, el cual se encuentra consagrado en el artículo 83 de la Constitución Política de 1991, y protege a las compañías aseguradoras. Este principio implica que la persona que decida firmar un contrato de seguros debe declarar con honestidad los hechos que puedan configurar un riesgo; es decir, debe responder con sinceridad el cuestionario que la aseguradora solicita; la falta de honestidad implicaría la nulidad del seguro y la retención de la prima por parte de la aseguradora (Decreto 410 de 1971, citado por Vásquez, 2017).

Así mismo, los siniestros causados intencionalmente no pueden invocar la posibilidad de un seguro; además, según el Código Penal (citado por Vásquez, 2017), se considera delito destruir, ocultar o deteriorar objetos asegurados para obtener un beneficio por parte de una aseguradora. De igual manera, la persona que cometa estas conductas puede ser judicializada por el delito de estafa, lo cual puede implicar una condena de entre cuatro y ocho años de prisión si el delito está relacionado con un contrato de seguros (Ley 599 de 2000, citada por Vásquez, 2017).

Como se puede evidenciar en las cifras mencionadas anteriormente, el fraude está presente en las diferentes industrias y ramas de la economía; de igual forma, impacta al sector asegurador en sus diferentes ramos. Es importante aclarar que en cada ramo el fraude tiene un comportamiento particular, y también se transforma adoptando nuevas modalidades de acuerdo con los cambios en el entorno; por tal razón, es fundamental diferenciar los indicadores en cada ramo y actualizarlos frecuentemente para garantizar su efectiva detección.

Para este caso particular, se abordará de manera general el fraude en transporte de mercancías, considerando la complejidad de la operación de este esquema de aseguramiento, regido por un marco normativo y de seguridad más exigente, derivado de la legislación internacional, que implica diferentes condiciones comerciales para las compañías.

El fraude en el transporte de mercancías

El seguro de transporte se define como el contrato en el cual una aseguradora asume el riesgo de indemnizar a una empresa por los daños o pérdidas de mercancía que puedan surgir durante el transporte aéreo, terrestre, fluvial o marítimo de ella; además, las pólizas suelen cubrir los gastos en los que el asegurado incurre para mantener el buen estado de las mercancías (Fasecolda, 2012).

De acuerdo con Fasecolda (2012), existen unas exclusiones para este seguro que se deben tener en cuenta antes de adquirir la póliza, con el fin de evitar hacer reclamaciones ilegítimas de manera no intencional por desconocimiento de estas:

- Pérdida de peso o volumen en las cantidades que se consideren normales.
- Pérdidas o daños que sean consecuencia de un empaque inadecuado.
- El dolo o culpa grave del propietario de la mercancía.
- Las pérdidas ocasionadas a causa de una mala gestión del propietario de la mercancía, la empresa transportadora o quien alquile el transporte, relacionada con la adquisición, transporte o entrega de ella.
- Los daños o pérdidas que sean causados por actos de guerra o por artefactos de guerra abandonados.
- Pérdidas que sean consecuencia de huelgas o actos mal intencionados.
- Envíos por correo postal.

La omisión de estas exclusiones a la hora de presentar una reclamación puede prestarse para diferentes acciones fraudulentas o delictivas, como:

Falsificación de mercancías: sucede cuando se contrata el servicio de transporte para movilizar imitaciones de mercancías ilegales; esta actividad tiene repercusiones económicas que superan los 250.000 millones de dólares (Oficina de las Naciones Unidas contra la Droga y el Delito - UNODC).

Lavado de activos a través del tráfico ilícito de mercancías: en ocasiones, los delincuentes intervienen la cadena de suministro para hacer blanqueo de dinero y poner a circular mercancía falsa involucrándose con el transporte de ella (UNODC).

Extorsión, corrupción y bandas criminales: la importación y exportación de productos falsificados ha permitido que las bandas criminales se lucren a través del transporte de estas imitaciones, utilizando el soborno y la corrupción para lograr distribuirlas internacionalmente (UNODC).

Evasión fiscal y arancelaria: evadir impuestos y derechos arancelarios cuando son de contrabando (UNODC).

Crimen organizado (online): se han desarrollado nuevas formas de defraudar a los compradores, donde la solicitud online del producto en muchas ocasiones no corresponde con el pedido realizado por el usuario, no llega a su destino, el que realizó el pedido es un delincuente que hurta la mercancía haciéndose pasar por una empresa fachada, entre otras modalidades (UNODC).

Hurto de mercancías: ocurre cuando durante el transporte de la mercancía, esta se roba o se apodera de ella forma ilícita; las modalidades son: auto hurto, suplantación de autoridades o de identidad, saqueo de contenedores, gemeleo o hurto por medio de correo electrónico (UNODC).

Estas tipologías de fraude han afectado a los diferentes actores, como tenderos, transportadores, empresas y compañías de seguros que amparan los riesgos asociados al transporte de las mercancías, lo que ha ocasionado pérdidas significativas y amenazas a su integridad física, considerando las acciones delictivas a las que acuden los delincuentes para lograr su cometido (UNODC).

Debido a los riesgos asociados al transporte, es importante mencionar que el artículo 986 del Código de Comercio (1971), sobre la pluralidad de transportadores: reglas para definir la responsabilidad, establece que son los transportadores quienes asumen la responsabilidad por la pérdida o daños a las mercancías durante el transporte de ellas, tal como se expone a continuación:

Cuando varios transportadores intervengan sucesivamente en la ejecución de un único contrato de transporte por uno o varios modos, o se emita billete, carta de porte, conocimiento de embarque o remesa terrestre de carga, únicos o directos, se observarán las siguientes reglas:

1. Los transportadores que intervengan serán solidariamente responsables del cumplimiento del contrato en su integridad, como si cada uno de ellos lo hubiere ejecutado.

2. Cada uno de los transportadores intermedios será responsable de los daños ocurridos durante el recorrido a su cuidado, sin perjuicio de lo previsto en la regla anterior.

3. Cualquiera de los transportadores que indemnice el daño de que sea responsable otro transportador, se subrogará en las acciones que contra este existan por causa de tal daño.

4. Si no pudiere determinarse el trayecto en el cual hayan ocurrido los daños, el transportador que los pague tendrá acción contra cada uno de los transportadores obligados al pago, en proporción al recorrido a cargo de cada cual, repartiéndose entre los responsables y en la misma proporción la cuota correspondiente al transportador insolvente.

A partir de esta legislación, se busca que el defraudador se cohíba de realizar acciones ilícitas asociadas al fraude en el seguro de transporte de mercancías, y también que los actores involucrados tomen medidas más rigurosas para evitar la comisión de este flagelo.

De igual forma, es fundamental conocer los indicadores asociados al fraude en el ramo de transportes, propuestos en la segunda edición del Manual de Indicadores Cualitativos de Fraude, elaborado por INIF (2007), los cuales se basaron en el análisis de casuística y se fundamentaron en los delitos asociados al fraude a los seguros. A continuación, se muestran los principales indicadores:

- Estadía de la carga en un parqueadero que no reúne las características de seguridad adecuadas.
- Cambio del cabezote y del conductor sin autorización del asegurado o transportador.
- Reportar varadas por fallas mecánicas al poco tiempo de iniciar el recorrido o en las afueras de la ciudad de destino.
- El camión y el conductor es un tercero, con una débil vinculación con el transportador, siendo este un empresario con débil capacidad económica industrial.
- El vehículo viaja sin escoltas, a pesar de estar en las garantías, o demuestra la deficiencia en la prestación de este servicio cuando se refiere a carga crítica.
- En la denuncia, el conductor aporta pocos detalles sobre la ocurrencia de los hechos y de la identidad del automotor.
- La denuncia se instaura días después de ocurrido el siniestro en otra población, especialmente en inspecciones de policía y no ante autoridades de policía judicial.
- El siniestro por accidente de tránsito y saqueo no deja huella de mercancías deterioradas o regadas en los alrededores.
- El siniestro por accidente de tránsito no deja huellas de frenadas o daños en zonas adyacentes que indiquen la real ocurrencia del hecho.
- El asegurado y el conductor manifiestan que la mercancía a granel se transportaba en un vehículo tipo camión, cuando se requiere un *container* o tanque de acuerdo con el producto.
- En el accidente de tránsito no se involucra otro vehículo, y si lo incluye, el asegurado y el conductor no saben la placa o características para ubicarlo.
- La ausencia de documentos que acrediten la idoneidad del conductor (licencia de conducción con la categoría correspondiente, carta de la empresa transportadora indicando que viene en representación de esta, autorización de la autoridad portuaria para ingreso).
- Las fechas de emisión de la remesa terrestre y el manifiesto de carga no corresponden con la fecha de ocurrencia del siniestro ni de la factura comercial.
- Difiere el valor entre lo declarado a la DIAN y el valor contenido en la factura comercial.

Vale la pena aclarar que los indicadores no necesariamente representan la consumación del fraude. Dependiendo de las políticas de la compañía, se recomienda que una vez identificados estos indicadores, se inicie una investigación más exhaustiva para confirmar las sospechas (INIF, 2007).

INIF, con base en su amplia experiencia en el fraude, apoya a las compañías de seguros y a las entidades judiciales y gubernamentales en la lucha contra este fenómeno, trabajando en la construcción de una cultura de honradez, así como la generación de conocimiento en técnicas y modalidades para empleados de las compañías y autoridades judiciales, que ayuden a cumplir los principios de prevención, detección y respuesta al fraude.

Para cumplir con este propósito, INIF desarrolla investigaciones que se rigen por los principios de transparencia, integridad, objetividad, rigurosidad y confidencialidad. Ellas han generado como resultado casos de estudio que permiten evidenciar diferentes modalidades y tendencias de fraude, que a su vez fortalecen las acciones de lucha contra este flagelo y han permitido evidenciar situaciones de riesgo que se deben tener en cuenta para contrarrestar las acciones cometidas por los delincuentes.

Recomendaciones para la prevención de fraude

- En virtud de lo anterior, INIF brinda las siguientes recomendaciones para mitigar o evitar el fraude en las organizaciones:
- Reconocer y comprender a fondo la dinámica general del fraude.
- Desarrollar programas de formación interna en prevención y detección del fraude.
- Construir indicadores de fraude.
- Realizar auditorías y evaluación de riesgos.
- Desarrollar y mantener actualizados los manuales y protocolos de tratamiento de fraudes detectados.
- Fomentar campañas de promoción de cultura antifraude.
- Establecer canales de denuncia y líneas éticas.
- Instaurar estrategias de inteligencia de negocios/Analitycs para la generación de modelos predictivos e índices de fraude.
- Perfilar al defraudador con base en sus características más relevantes.
- Practicar procesos antifraude de control y selección de personal.

Buscamos que estas recomendaciones sean una herramienta para fortalecer las políticas antifraude dentro de las compañías, aclarando que cada una de ellas debe ser revisada y adaptada a las características particulares de cada empresa. De igual forma, lo más importante es promover una cultura de honradez caracterizada por la ética, la integridad y las buenas prácticas, que permitan construir un entorno comercial confiable, comenzando desde el interior de la organización y expandiéndose a los demás grupos de interés, impactando y creando una sociedad más honesta en Colombia.

Referencias

Alexopoulos, P., Kafentzis, K., Benetou, X., Tagaris, T. & Georgolios, P. (2007). Towards a Generic Fraud Ontology in e-Government. In ICE-B (pp. 269-276). Recuperado de: https://bit.ly/2mWaFRA

Association of Certified Fraud Examiners (2014-2018). ¿Qué es el fraude? ACFE. Recuperado de: https://bit.ly/2Fepc1r

Ayuso, M. (1998). *Modelos econométricos para la detección del fraude en el seguro del automóvil* (pp. 1-10). Universidad de Barcelona.

Borda, C. (2015). *Importancia relativa de los factores de riesgo de fraude para los auditores de Colombia* (pp. 1-123). Universidad Nacional de Colombia. Facultad de Ciencias Económicas, Escuela de Administración y Contaduría Pública.

Coalition Against Insurance Fraud. Fraude de seguro: el delito que paga usted. Recuperado de: https://bit.ly/2IprcNr

De la Espriella, C. (2012). Fraude en seguros. *Una aproximación al caso colombiano* (pp. 561-595). Fasecolda.

Dellaportas, S. (2013). Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. *Accounting Forum, 37* (7): 29-39.

EY - Ernst & Young. La integridad en las primeras planas: El futuro del "Compliance". 15.ª *Encuesta Global sobre Integridad en los Negocios 2018* (pp. 1-28). EY Building a better working world.

Federación de Aseguradores Colombianos (2016). Acción abril 28 2016: La banca y aseguradoras, en alerta por estafas con pagos por internet. Recuperado de: http://bit.ly/2YVRFVw

Federación de Aseguradores Colombianos (2012). Seguro de transporte (pp. 1-24). Fasecolda.

Fernández, L., Niño, F. & Cabrera, J. (2005). El fraude a los seguros. *Revista Criminalidad, N.º 48.* Capítulo V: Lo local y el crimen organizado, pp. 349-357.

Galvis, I. E. & Santos-Mera, J. E. (2017). Geometría del fraude. *Cuadernos de Contabilidad, 18* (45): 74-85.

INIF - Instituto Nacional de Investigación y Prevención de Fraude (2007). Manual de indicadores cualitativos de fraude. *INIF (2), 1: 1-10.*

INIF - Instituto Nacional de Investigación y Prevención de Fraude (2015). Manual de políticas y procedimientos de un plan antifraude. Documento no publicado, INIF, pp. 1-25.

INIF - Instituto Nacional de Investigación y Prevención de Fraude (2017). Gestión analítica: cifras detección de fraude 2017. Documento no publicado, INIF, pp. 1-10.

INIF - Instituto Nacional de Investigación y Prevención de Fraude (2018a). Ciclo de análisis de fraude: cartillas de detección y prevención. INIF, pp. 1-16.

INIF - Instituto Nacional de Investigación y Prevención de Fraude (2018b). Gestión analítica: cifras detección de fraude 2018. INIF, pp. 1-10.

KPMG (2017). Encuesta de Fraude en Colombia 2017. KPMG Colombia, pp. 1-17.

KPMG (2018). Y su empresa: ¿Está blindada contra la corrupción? KPMG, pp. 1-17.

Kroll Advisory Solution en el año 2012. Informe Global sobre Fraude. Kroll, pp. 1-64.

Ley 599 de 2000. Código Penal, Colombia, 24 de julio del 2000.

Lokanan, M. (2015). Challenges to the fraud triangle: Questions on its usefulness. *Accounting Forum, 39: 201-224.*

López, W. & Sánchez, J. (2012). El triángulo del fraude. *Forum Empresarial, 17* (1): 65-81.

Nájera, A. (2019). Boletín de estadísticas n.° 008-2019: Resumen de los resultados preliminares de la industria aseguradora y de capitalización al cierre del año 2018. Fasecolda, pp. 1-10.

NIA-ES 240 - Norma Internacional de Auditoría 240 (2013). Responsabilidades del auditor en la auditoría de estados financieros con respecto al fraude (NIA-ES 240). España, 15 de octubre de 2013. Recuperado de: https://bit.ly/2XppHwI

Price Benowitz LLP (2017). White Collar Attorneys: Fraude. Recuperado de https://bit.ly/2mPpEwq

PwC - PricewaterhouseCoopers (2016). Encuesta Global Sobre Delitos Económicos y Fraude 2018. Capítulo Colombia: Hacia una nueva ética en los negocios: preparados para evitar el crimen económico y cibernético. PwC, pp. 1-44.

PwC - PricewaterhouseCoopers (2018a). Comunicado de prensa: El crimen económico global reportado alcanza niveles récord; aumenta la preocupación por los delitos cibernéticos, costos y la responsabilidad, pp. 1-4. Recuperado de: https://www.pwc.com/ia/es/prensa/pdfs/gecs-2018-pwc.pdf

PwC - PricewaterhouseCoopers (2018b). Encuesta mundial sobre fraude y delito económico 2018. PwC. Recuperado de https://www.pwc.es/es/forensic-services/encuesta-mundial-fraude-delito-economico-2018.html

PwC - PricewaterhouseCoopers (2018c). Encuesta Global Sobre Delitos Económicos y Fraude 2018. Capítulo Perú. PwC, pp. 1-16.

PwC - PricewaterhouseCoopers (2018d). Encuesta Global Sobre Delitos Económicos y Fraude 2018. Capítulo Colombia: Fraude al descubierto. PwC, pp. 1-44.

PwC - PricewaterhouseCoopers (2018e). Encuesta Global sobre Delitos Económicos 2018. Capítulo México. PwC. Recuperado de https://www.pwc.com/mx/es/prensa/comunicados-prensa/encuesta-de-delitos-economicos-2018-edicion-mexico.html

Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. Issues in *Accounting Education, 23 (4): 521-533.*

Rodríguez, M. & Gartner, I. (2017). The Cressey hypothesis (1953) and an investigation into the occurrence of corporate fraud: an empirical analysis conducted in Brazilian banking institutions. *Revista Contabilidade & Finanças, 29 (7): 60-81.*

Schuchter, A. & Levi, M. (2015). Beyond the fraud triangle: Swiss and Austrian elite fraudsters. *Accounting Forum, 39: 176-187.*

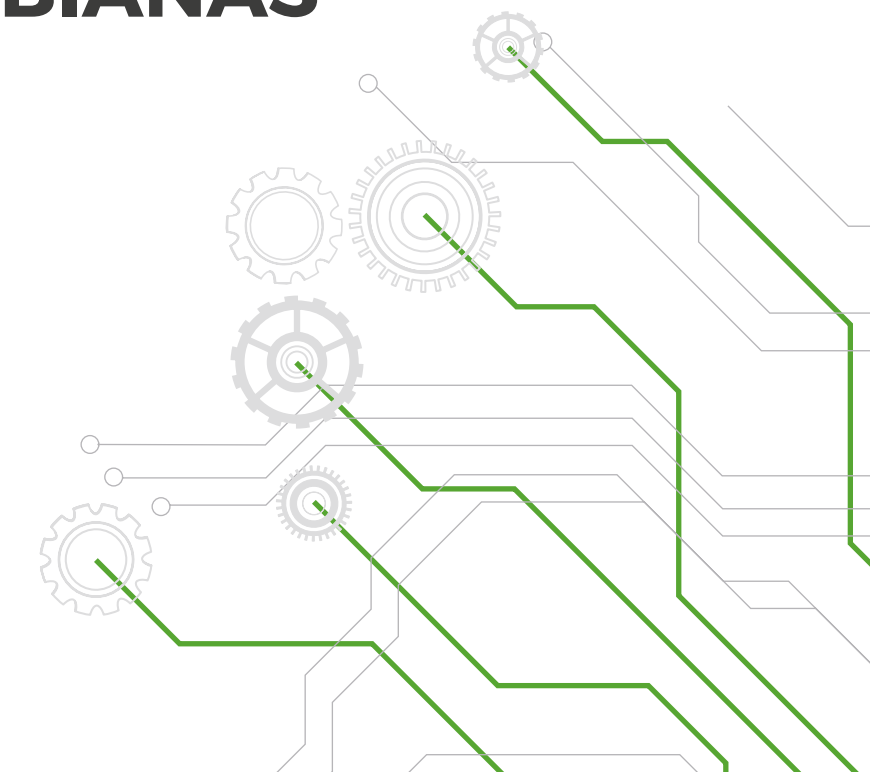
Silva, J. & Nájera, A. (2015). Resultados de la industria aseguradora en el año 2015. Fasecolda, pp. 34-40.

Vásquez, D. (2017). La mala fe y el fraude en el derecho colombiano de seguros. *Revista Ibero-Latinoamericana de Seguros, 46:* 15-35.

Wolfe, D. & Hermanson, R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal.*

CAPÍTULO 5

GUÍA PRÁCTICA PARA LA CIBERSEGURIDAD EN LAS EMPRESAS COLOMBIANAS



5. Guía práctica para la ciberseguridad en las empresas colombianas

Por: Coronel (RA) Fredy Bautista García
Consultor Ciberseguridad

Los cibercriminales se han convertido en una de las principales amenazas a la seguridad empresarial en el mundo, y las pérdidas derivadas de los ciberataques ya superan las generadas por los riesgos tradicionales, como fraudes internos o incluso eventos inesperados, como son los desastres naturales.

La tendencia y el comportamiento de estas estructuras delictivas demuestran el alto nivel de sofisticación y, por ende, la tasa de éxito con la que consiguen vulnerar la seguridad de las empresas crece anualmente.

Esto sucede, en gran medida, porque los recursos con los que cuenta el cibercrimen permiten a sus integrantes asociarse con el crimen organizado en una relación de beneficios mutuales, entre otros:

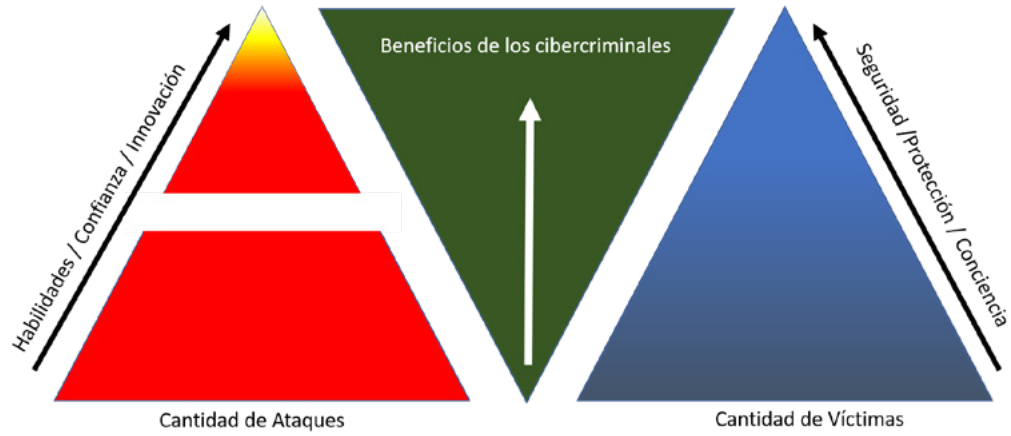
- Anonimización de los delincuentes
- Innovadores esquemas de ciberlavado
- Protección y seguridad a integrantes
- Tráfico de datos
- Compra de información sensible de las empresas
- Preparación de ataques a la medida
- Reclutamiento de empleados (insiders)

Las habilidades de los cibercriminales guardan una relación directa con los beneficios económicos de un ciberataque y el volumen de las empresas víctimas, según su nivel de conciencia, protección y seguridad.

Este modelo, denominado Tricotomía del Cibercrimen, útil para diseñar e implementar estrategias de ciberseguridad, fue incluido en el 2017 en el Informe de evaluación de amenazas en internet de Europol IOCTA.

La pirámide roja caracteriza a los delincuentes, entre los que se incluye una amplia base de atacantes con una baja capacidad técnica, que, no obstante, pueden comprar el acceso a las habilidades y herramientas de las que carecen (crimen como servicio).

En este nivel hay poca o ninguna innovación, y los cibercriminales utilizan solo herramientas existentes y de métodos conocidos.



No obstante, a medida que aumentan las habilidades también lo hacen los niveles de innovación, y con ello los requisitos fiduciarios para los cibercriminales al trabajar cada vez más en colaboración.

Por último, en la parte superior de la pirámide de ataques se encuentra el grupo integrado por personal altamente calificado, individuos que existen dentro de pequeños círculos de confianza y donde está el verdadero potencial de innovación de los criminales.

En este escenario también se destaca el techo de habilidad, desde donde los cibercriminales ya no pueden comprar herramientas para elevar su progresión; por ende, evolucionan y desarrollan sus propias habilidades.

La pirámide azul representa el volumen de víctimas (ciudadanos / organizaciones / empresas). Aquí se cuenta con una amplia base de las víctimas que carecen de la competencia técnica o de seguridad y de la conciencia necesaria para protegerse suficientemente a sí mismos.

Igualmente, en la parte superior de la pirámide se encuentra un menor número de víctimas potenciales que han alcanzado un alto nivel de seguridad, y por lo tanto, los ataques que suelen tener una significativa tasa de éxito menor.

También es claro que, según el valor de los activos y la voluntad de invertir en programas de ciberseguridad, puede aumentar el riesgo de un ciberataque exitoso.

Respecto a las ganancias percibidas, la pirámide verde representa los beneficios o ganancias potenciales por ataque. Como regla general, los ataques más sofisticados y organizados son capaces de perseguir objetivos de alto valor (grandes compañías), que suelen tener una mayor seguridad en su ciberentorno, por lo que los criminales obtendrán mayores beneficios monetarios e intrínsecos.

Debe indicarse, igualmente, que existe un gran número de pequeñas empresas que se convierten en blanco de múltiples organizaciones delictivas, a las cuales, sin importar el monto de las ganancias posibles, apuntan sus ataques a una masa crítica empresarial desprotegida.

Ciberataques más frecuentes en las empresas colombianas

Sin importar el tamaño de las empresas, los informes sobre el estado del cibercrimen en el país establecen los cinco ciberataques más frecuentes que afectan a las empresas colombianas:

- *Ransomware*
- Fraude BEC
- Robo de identidad
- *Phishing*
- Fuga de datos

Todos estos ataques se encuentran asociados a múltiples factores vinculados a la problemática de inseguridad en ciberentornos empresariales:

- Escaso nivel de concienciación por parte de directivos-empleados.
- Débil implementación de políticas de ciberseguridad.
- Priorización de otros riesgos por encima del cibernético.
- Obsolescencia tecnológica en las plataformas.
- Descoordinación entre las áreas de seguridad física y tecnológica.
- Exposición de información sensible empresarial en internet.
- Desconocimiento del actual nivel de riesgo de la compañía.
- Inexistencia de un estudio del estado actual de la ciberseguridad de la empresa.
- Estructuras organizativas desactualizadas o inexistencia de áreas, cargos y responsabilidades frente a la ciberseguridad.

Todos estos factores facilitan el actuar delictivo de los criminales, que encuentran a las organizaciones expuestas tanto en el escenario técnico y humano como de procedimientos, y esto les permite concretar con éxito su actividad delictiva.

Implementación de políticas de seguridad

Es necesario que todas las organizaciones, sin importar su tamaño o valor de sus activos, adopten políticas de seguridad que permitan mejorar los procesos internos y ayuden a mitigar el impacto por fallas en la ciberseguridad.

Esas políticas pueden ser implementadas con la adopción de planes que involucren desde directivos, el equipo técnico y, en general, a todos los empleados de la organización, incluso contratistas y otras partes involucradas en la cadena productiva de cada empresa, así como la relación con clientes y proveedores, entre otros.

Algunas de las políticas que deben ser implementadas en las empresas, a fin de enfrentar las ciberamenazas, son las siguientes:

Política de recursos humanos

La política asociada a la gestión de RR. HH. respecto a la ciberseguridad responde a uno de los mayores desafíos que tienen las empresas en Colombia, pues el factor humano puede evitar, a través de adecuadas prácticas, muchos incidentes.

El objetivo primordial de la política de recursos humanos es asegurar que todo el personal que se encuentra involucrado en la actividad de negocio de una empresa conozca los derechos, los deberes y las responsabilidades que le asisten en torno a su relación con la seguridad de la información. Por lo tanto, es importante que las empresas definan, igualmente, mecanismos sancionatorios ante comportamientos negligentes que pongan en riesgo los principales activos de información de una organización.

Dentro de los controles que establece esta política se destacan los siguientes:

Cláusulas contractuales: los contratos laborales de los empleados deben considerar aspectos importantes relativos a la ciberseguridad.
Acuerdo de confidencialidad: se deben suscribir acuerdos de confidencialidad que establezcan la manera como los empleados pueden acceder a la información sensible.
Revisión de candidatos: antes de la contratación se deben revisar las referencias de los empleados y los candidatos, con el fin de establecer sus antecedentes.
Planes de formación y concienciación: la empresa debe disponer de un plan de formación y concienciación en ciberseguridad.
Compromiso de la alta dirección en las jornadas de concienciación. La política debe comprometer a los directivos, los que deben acompañar activamente estas actividades.

Esta política debe contemplar sanciones y el procedimiento que se va a seguir cuando se presenten usos negligentes de información sensible de la empresa o la finalización de un contrato, para garantizar la seguridad de sus activos de información.

Las empresas deben disponer de una adecuada política de permisos y de privilegios, con el fin de evitar accesos no convenientes, y cancelar los usuarios en casos de vacaciones, permisos y finalización de contrato.

Los anteriores compromisos resultan muy importantes teniendo en cuenta una oportuna concienciación, lo que permite disminuir la tasa de éxito de los ciberataques.

Una vez que las empresas han establecido las normas en torno al recurso humano, es importante que se definan aspectos relativos al almacenamiento de información en las redes corporativas.

Política relativa al almacenamiento de información

Esta política tiene como objetivo conseguir que los empleados hagan un buen uso de los servicios de almacenamiento, además de un óptimo tratamiento de la información.

- Dentro de las ventajas de esta política podemos enunciar:
- Sensibilización de los empleados para prevenir la pérdida de documentos
- Centralización de las copias de seguridad
- Realización del respaldo de la información
- Participación de varios empleados en proyectos comunes al compartir de manera adecuada la información
- Optimización del uso de los servidores de almacenamiento al evitar duplicidades en información, entre otras.

Esta política facilita a las empresas:

- Informar oportunamente a los empleados sobre los servicios de almacenamiento disponibles.
- Notificar a los empleados sobre la información que se comparte, los datos que se almacenan y la responsabilidad que ello conlleva.
- Dar claridad a los empleados sobre el tiempo de almacenamiento de la información y cuándo esta se puede eliminar.
- Informar oportunamente a los empleados sobre la política de clasificación de la información y los aspectos relativos a su eliminación de la red corporativa.
- Implementar reglas de acceso a la información para controlar quién accede, a qué dispositivo y a cada disco de almacenamiento.
- Establecer una política clara respecto a las copias de seguridad, para determinar cada cuánto tiempo se deben realizar, dónde se almacenan y el tiempo que se van a conservar sus copias.
- Definir el acceso a los empleados solo si es necesario para desempeñar su trabajo.
- Revisar periódicamente el estado de los servidores y su capacidad, así como el registro de la estadística de uso, los usuarios habilitados para acceder y el estado de la información crítica almacenada en los servidores.

Es muy importante establecer una política para fijar los lineamientos de la empresa respecto al almacenamiento de información en los equipos de trabajo, dada la utilización de diferentes dispositivos, como computadores portátiles, de escritorio, tabletas, teléfonos celulares y demás.

El uso de estos dispositivos genera y transmite información necesaria para el desempeño de la función del empleado, y esta información, a veces, es

almacenada en los discos locales de estos equipos; por lo tanto, es necesario tener una política que garantice que el almacenamiento y tratamiento se hará de manera segura.

Esta política de almacenamiento en dispositivos tendrá alcance a dispositivos extraíbles, como USB o discos externos, al igual que el almacenamiento en la nube.

El objetivo principal de la política de almacenamiento de información de los equipos de trabajo permite especificar las reglas, criterios y procedimientos que se deben seguir por parte de los empleados; en este sentido, las empresas deben adoptar los siguientes controles:

- Elaborar una normativa para controlar el almacenamiento de información en los equipos corporativos.
- Informar a los empleados sobre dónde guardar la información generada en su equipo de trabajo, directorio de carpetas, subcarpetas, archivos, etc.
- Establecer el tiempo de conservación de la información que estará disponible de forma local.
- Dar claridad sobre qué información se podrá transferir a los servidores y cuál se eliminará.
- Cifrar la información de carácter crítico y sensible antes de ser guardada de manera local.

Respecto a la información que se puede almacenar localmente, la política deberá especificar qué no se debe guardar de este modo en el equipo, como documentos o fotografías personales, archivos de música, entre otros.

Es importante distinguir también aquellos archivos que se descargan de internet y que pudieran estar protegidos por normas de derechos de autor.

Ahora bien, frente al cifrado de la información, se debe sensibilizar a los empleados de los casos de robo de esta por pérdida de dispositivos, y la necesidad de asegurar la confidencialidad de la información en estos casos. Inclusive, se puede optar por disponer de tecnología que permita eliminar de manera remota dicha información.

Una adecuada **POLÍTICA SOBRE COPIAS DE SEGURIDAD** o respaldos de información resulta muy útil para mitigar el impacto por ataques de *ransomware* y facilitar un sistema de recuperación. Se deben considerar las siguientes pautas:

Asignar responsabilidad y autoridad: la seguridad del almacenamiento debe convertirse en una función dentro de la arquitectura y las políticas globales de seguridad de la información.

Establecer la frecuencia de las copias de seguridad: hay que tener en cuenta que desde el último respaldo realizado es que se podrá hacer la recuperación de datos de la plataforma tecnológica.

Definir los tipos de *back-up:* la copia de seguridad puede realizarse en distintas modalidades, ya que se pueden emplear **copias completas, diferenciales e incrementales.** Las completas contemplan la copia de toda la información, y las diferenciales solo copias de la información que ha sufrido cambios desde el último respaldo.

Plan de recuperación de datos: se deben fijar responsabilidades para este proceso, asignando funciones para la puesta en marcha de este plan en caso de ser requerido.

Almacenamiento en la nube

La nube se ha convertido en una opción válida para almacenar información, optimizar el uso de recursos locales, ampliar las posibilidades de acceso remoto a la información y reducir los costos para la operación de las compañías.

Por ende, es muy importante para las organizaciones establecer de manera clara cuáles son los casos en los que se puede permitir el almacenamiento de información, y de esta manera fijar las reglas, criterios y procedimientos que se deben seguir por parte de los empleados.

A continuación presentaremos una lista de actividades para la implementación adecuada de una política de almacenamiento y gestión de información en la nube.

- Informar a los empleados sobre si es permitido o no el uso de servicios de almacenamiento de información en nubes públicas, como Dropbox, One Drive, Google Drive, entre otros.
- Diseñar una lista, en donde los empleados pueden consultar qué servicios de almacenamiento en la nube están permitidos y cuáles no.
- Realizar jornadas de capacitación al personal sobre el procedimiento de borrado seguro de la información almacenada en la nube.
- Dar a conocer a los empleados el tipo de información que se puede almacenar en la nube y si necesita ser cifrada o no.
- Establecer un mecanismo para valorar las ventajas o inconveniencias de almacenar información y copia de seguridad en la nube.
- Definir los requerimientos mínimos legales para el adecuado funcionamiento del servicio de la nube por parte de los responsables de la contratación de los servicios.
- Establecer la conveniencia de incluir la gestión de incidentes informáticos y servicios forenses.
- Dar claridad a la controversia que pudiera presentarse por el tratamiento de datos de terceros (clientes) en servicios de almacenamiento en la nube.

Política de aplicaciones permitidas en dispositivos de la empresa

Esta política permite conocer el *software* y las aplicaciones utilizadas por la empresa, y prevenir los ciberataques por vulnerabilidades en estos servicios; además, establece si estos servicios se han adquirido de manera legal, lo cual mitiga riesgos de litigios por usos no autorizados.

Dentro de los controles propuestos, la empresa debe mantener un registro actualizado de la licencia disponible del *software* autorizado; además, se recomienda:

- Nombrar personal técnico debidamente capacitado para encargarse de la instalación y actualización del *software* en la empresa.
- Definir el procedimiento de eliminación del *software*, cuando producto de la auditoría se detecten usos no autorizados.
- Notificar al personal sobre las sanciones que se pueden derivar por el uso de programas no autorizados.
- Disponer de un repositorio, donde se encuentre todo el *software* que está autorizado, con su debida licencia o credencial de instalación.

Sobre el registro de las licencias, es importante conocer:

- Nombre
- Versión del producto que ha sido licenciado
- Cuándo se adquirió
- Planes de renovación de esta licencia
- Número de usuarios que están permitidos por licencia

- Realizar auditorías periódicas del *software* instalado, con el fin de identificar usos no autorizados o aplicaciones potencialmente riesgosas.
- Evitar el uso de programas sin autorización o sin actualización, los cuales suponen riesgos adicionales a la seguridad de la información.
- Mantener disponible la facturación o comprobantes que demuestren la adquisición legal de dichos productos.

En los últimos años algunas empresas han utilizado el modelo de política **BYOD** *(Bring Your Own Device)*, que busca solucionar los conflictos que se puedan derivar por el uso de los dispositivos propios de los empleados en el entorno empresarial.

Y aunque se requiera acceder a la información de la empresa, se necesita su protección, buscando un equilibrio entre la productividad y la seguridad.

Por lo anterior, es necesario asegurar los teléfonos móviles y las tabletas, e identificar las aplicaciones que potencialmente podrían influir en aspectos asociados con aumentar el uso productivo de estos dispositivos y reducir el tiempo perdido.

Las empresas deben reservarse el derecho de auditar el acceso a la información, y los empleados, ser conscientes de que será muy difícil garantizar una expectativa de privacidad cuando se utiliza un correo corporativo o si la factura del teléfono es con cargo a la empresa. Cualquier política de este tipo deberá considerar los siguientes aspectos:

- Utilizar contraseñas fuertes y alfanuméricas.
- Emplear diferentes sistemas o métodos de autenticación para el acceso a estos dispositivos: utilización de contraseñas, validación biométrica.
- Establecer tiempos mínimos para bloqueos de accesos en caso de inactividad del dispositivo móvil.
- Definir a quién pertenecen los datos y las aplicaciones instaladas.
- Dejar claro qué sucede cuando un dispositivo se pierde o es robado.
- Establecer qué tipo de dispositivos están autorizados, qué aplicaciones se permitirán o prohibirán, y qué sitios web podrán ser bloqueados.
- Utilizar VPN y *software* de acceso remoto debidamente autorizados.
- Notificar la sanción en caso de que un empleado transmita material inapropiado por sus dispositivos personales utilizando una red de la empresa.
- Definir el nivel de soporte técnico para los dispositivos, respecto a quién deberá prestarlo y suministrarlo.
- Implementar una mesa de ayuda para la configuración de estos dispositivos.

La política, igualmente, debe explorar con claridad cómo se eliminará el acceso a la información de la empresa y al correo electrónico en el dispositivo del empleado, una vez que este deje la compañía, y el mecanismo mediante el cual se puede hacer una copia de la información, salvaguardando aquella del resorte personal e íntimo del empleado.

Recomendaciones para el uso de dispositivos móviles

Mantener actualizados los dispositivos móviles: las empresas fabricantes y desarrolladoras de los sistemas operativos para dispositivos móviles están publicando actualizaciones permanentes.

Impedir el uso de dispositivos con *jailbreak:* estas modificaciones a los estados originales de los teléfonos facilitan la instalación de aplicaciones no reguladas que pueden contener programas malignos.

Utilizar consola de administraciones de aplicaciones y dispositivos móviles: permiten realizar un inventario del *software*.

Política de clasificación de la información

Sin importar el formato de la información, que puede ser digital o de otro soporte, como papel, fotografías, videos, etc., es importante que las organizaciones incrementen sus esfuerzos para proteger adecuadamente la información.

Para ello, deben disponer de un inventario de estos activos y clasificarlos según el impacto que sufriría la empresa por la pérdida o el acceso no autorizado por una fuga, destrucción o alteración de la información, según criterios de confidencialidad, integridad y disponibilidad.

Estos criterios señalan, por ejemplo, que nadie debe tener acceso a la información si no está autorizado o que ella debe permanecer sin que sufra daños no deliberados, además de garantizar su disponibilidad, sin importar el tiempo transcurrido desde su almacenamiento y tratamiento.

Política de concienciación de la información

Es necesario que las compañías diseñen programas de concienciación sobre los riesgos cibernéticos asociados con su operación; todos los empleados deben conocer y aplicar las prácticas para el adecuado uso de los dispositivos digitales, la utilización de servicios en la web y en la nube, las redes sociales y el correo electrónico, entre otros.

Los programas de formación continua en ciberseguridad deben abarcar diferentes roles en la organización, pero garantizando siempre el compromiso de la alta dirección, de tal manera que todos entiendan y cumplan las normas y medios de protección en la materia, además de los riesgos por el incumplimiento o mal uso de los dispositivos digitales, así como las sanciones por violaciones a la política.

Las empresas deben documentar y difundir la norma de ciberseguridad y asegurar el acceso a todos los empleados.

- Elaborar y revisar el plan de formación, para elevar el nivel de seguridad de toda la plantilla de personal.
- Llevar el registro de la asistencia y participación, y en caso de requerirse, la aprobación de los cursos y charlas de concienciación en ciberseguridad, estableciendo una periodicidad que certifique la actualización de los empleados sobre los riesgos cibernéticos.
- Comprobar la asimilación del conocimiento adquirido, mediante la realización de auditorías internas para todos los empleados.

Todos estos aspectos apuntan hacia la implementación y apropiación de una cultura de ciberseguridad, que debe ser aplicada a toda la cadena productiva, inclusive los clientes y los proveedores.

Dado el impacto actual que se viene presentando con el crecimiento de los casos de fraude asociados a la estafa del CEO o fraude BEC, es prioritario que las empresas revisen su relación con los clientes y los proveedores, y tener en cuenta las siguientes recomendaciones:

1. Aplicar una política de privacidad, a través de la cual se informe a los clientes y proveedores el tratamiento que se le dará a la información recolectada, así como su utilización.
2. Tener claridad respecto al tratamiento de los datos e información de los clientes, dónde se almacenan, cómo se utilizan, quién accede a ellos y cómo se protegen.

Se debe realizar un ejercicio para eliminar la información antigua de clientes y proveedores, así como establecer los mecanismos de actualización de la información, acordándolos previamente con ellos.

Debe existir una normativa clara hacia clientes y proveedores, en la cual quede por sentado que no se cambiarán las condiciones de entrega de mercancías ni de pagos sin que se notifique previamente, y se agoten todos los mecanismos posibles de verificación y validación necesarios.

Igualmente, deben establecerse equipos de trabajo conjunto entre las áreas comerciales, de producción y financieras, en particular sobre los procesos de cobro de cartera y despachos de productos, para evitar ser víctima de engaños por parte de criminales, y fijar los procedimientos, roles y responsabilidades en la aplicación de controles, antes de realizar pagos a proveedores o gestionar cartera de los clientes.

Desde el punto de vista tecnológico, es importante que las empresas instituyan filtros que permitan bloquear ataques dirigidos con correos electrónicos, que suplantan a empresas clientes, mediante técnicas de *phishing* o *Mail Spoofing*.

En el mismo sentido, debe revisarse la información puesta o disponible de las empresas en internet, pues en ocasiones una inadecuada política de borrado de metadatos deja a merced de los criminales o delincuentes información valiosa, que facilita la configuración de ataques futuros.

Estas políticas están encaminadas a la gestión de la ciberseguridad por parte del empresario; sin embargo, las áreas técnicas deben efectuar controles que abarquen las siguientes pautas:

1. Control de dispositivos extraíbles, así como el almacenamiento de información en discos externos.
2. Control de cumplimiento de una norma obligatoria de cifrado almacenada en portátiles, celulares y almacenamiento en la nube.
3. Control de la política de escaneo y uso de programas de protección, como antivirus, antes de utilizar USB en los servidores y computadores de la organización.
4. Control de las descargas de información, en particular archivos en formatos que dificulten la detección de programas maliciosos, como extensiones .rar, .exe, etc.
5. Control de la disposición final de los dispositivos cuando se renuevan los equipos, implementando políticas de borrado seguro.

El borrado de información, en todo caso, deberá ser realizado por personal técnico idóneo, mediante la utilización de estándares de borrado ya establecidos internacionalmente.

Por otra parte, las compañías deben adoptar como buena práctica la realización de auditorías de sistemas de manera periódica, e identificar los activos más relevantes susceptibles del proceso de auditoría.

Las auditorías de sistemas deben estar enfocadas a la mejora continua y garantizar el avance del nivel de madurez en ciberseguridad de la organización.

Estas auditorías deben abarcar aspectos de tipo legal para medir el nivel de cumplimiento de normativas recientes sobre la protección del dato informático, tratamiento de datos personales, reportes obligatorios a entidades de control, entre otros.

Finalmente, es importante abordar la definición de una **POLÍTICA DE RESPUESTA A INCIDENTES** que compendie cómo debe reaccionar una organización frente a un ciberataque, y determinar las personas que se encuentran involucradas en la respuesta a incidentes; además, esta normativa ayuda a las empresas a:

- Determinar el nivel de responsabilidad de cada involucrado.
- Establecer el canal de comunicación oportuno y las tareas que se deben cumplir.
- Anticipar el servicio de proveedores externos de análisis forense (registro de logs), para la interpretación de la información durante las fases del incidente: antes, durante y después.
- Relacionar las tareas con el **plan de contingencia** de las organizaciones.
- Seleccionar el equipo capacitado que se encargará de gestionar un incidente sobre seguridad.

Este equipo debe estar en condiciones de usar apropiadamente la información que se recolecta en la gestión del incidente, para poder tomar las medidas con el fin de mejorar la seguridad del sistema afectado.

Los planes de gestión de incidentes deben ser sometidos a revisiones periódicas por parte de la alta dirección, y definir un catálogo de las situaciones o eventos que se consideran como incidente de ciberseguridad y que afectan directamente los activos y la cadena productiva de la empresa, según la criticidad aprobada.

Como vemos, todas estas políticas conllevan un alto compromiso de la alta dirección, y se hacen transversales a los diferentes roles y cargos dentro una empresa, sin importar su tamaño, pues como bien conocemos, cualquier organización puede ser víctima de un ciberataque.

Por lo tanto, es importante que las empresas consideren la reestructuración de sus organigramas e implementen cargos y funciones nuevas dentro de la estructura, como jefes de ciberseguridad, responsables de ciberseguridad o gestor de la ciberseguridad, de acuerdo con los parámetros establecidos en el estándar ISO 27032 2018.

Sin importar el estado o nivel de madurez del modelo de ciberseguridad, todas las empresas deben considerar como buena práctica reportar los incidentes informáticos al CAI Virtual de la Policía Nacional en su canal de denuncia caivirtual.policia.gov.co.

CAPÍTULO 6

LA GESTIÓN DE LA SEGURIDAD Y EL IMPACTO DE LA CUARTA REVOLUCIÓN INDUSTRIAL EN LA CADENA DE SUMINISTRO

6.1. Gestionando la seguridad, una responsabilidad empresarial

Por: John Jairo Mónoga G.

El sueño de un empresario es crear y conformar una compañía que le permita llevar a cabo las actividades que más le gusta realizar e, igualmente, tener una independencia económica.

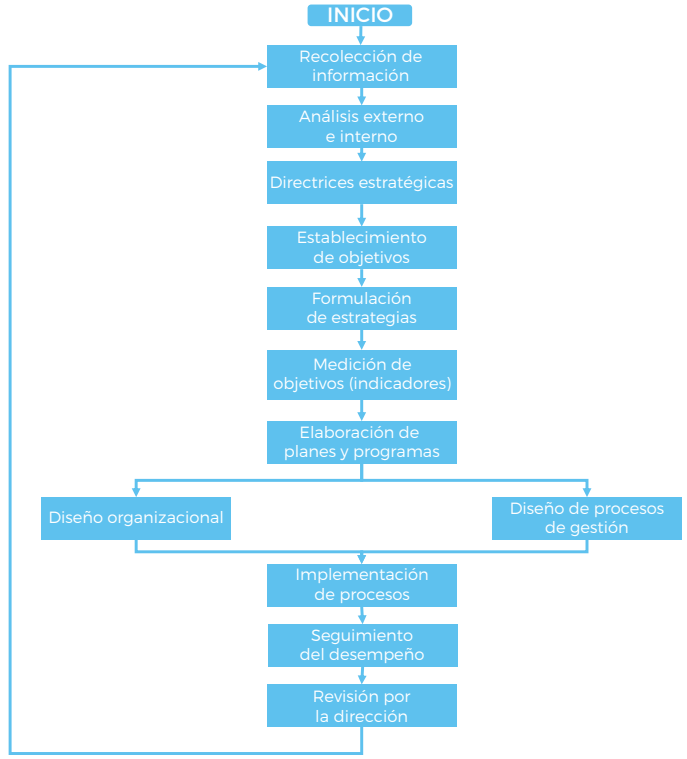
Al trazar este sueño se identifican objetivos organizacionales, los cuales quieren ser logrados en el menor tiempo posible.

Por eso, es necesario determinar el rumbo que se debe seguir, conocimiento de cuál es el "querer ser" de la empresa, cuál es su razón de ser y qué segmento o mercado pretende cubrir.

Para conocer esto es necesario partir de la planeación estratégica, que genera a su vez el direccionamiento estratégico para determinar la forma de actuar.

La organización que quiera construir la planeación estratégica debe conocer su entorno, dónde está ubicada y con quién interactúa, quiénes son sus competidores y cuáles los productos o servicios que ofrece, y cuál es la percepción del cliente final; sobra la oferta del mercado a partir del mercado, y desde esa percepción, establecer qué parte de ese mercado quiere cubrir. Cuáles son los productos y servicios con lo que quiere competir y cuáles son las necesidades que se quiere satisfacer.

En la siguiente gráfica se determinan las etapas en la planeación estratégica, para que así la organización defina su modelo de negocio (tomado de *Indicadores de gestión*, Icontec).



A medida que el empresario avanza, va creando la "propuesta de valor", la cual determina y describe el conjunto de beneficios que la organización ofrece a sus clientes, teniendo en cuenta un precio atractivo, cualidades del producto y servicio, así como beneficios explícitos que recibe al adquirirlos.

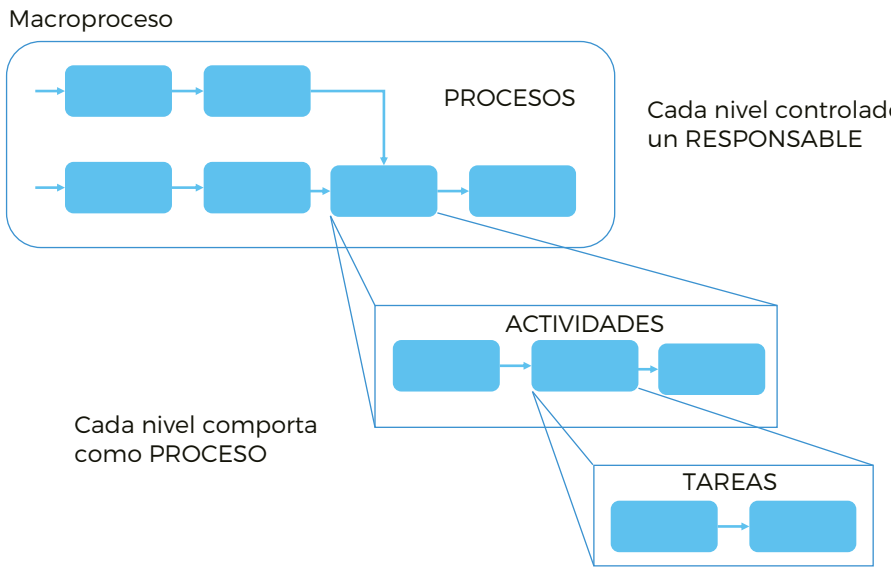
En esa cadena de valor, la organización diseña y establece los procesos que le aportarán y ayudarán a lograr los objetivos propuestos inicialmente; algunos de ellos pueden ser:

- Comerciales, para captar clientes y cumplir las metas de la ventas.
- Compras, para adquirir bienes y/o servicios.
- Recursos humanos, para identificar y seleccionar personal idóneo y calificado.
- Financieros, para la administración eficiente de los recursos.
- Servicio al cliente, para conocer las necesidades y cumplimiento de los clientes.
- Calidad, para mejorar el desempeño del producto y servicio, así como la optimización de los procesos.
- Manufactura, para producir los productos con base en los requerimientos del cliente.

- Logística y distribución, para ubicarlos en las condiciones y tiempo requeridos.
- Tecnología, para contar con la infraestructura y equipo que le permitan el manejo de información.
- Entre otros.

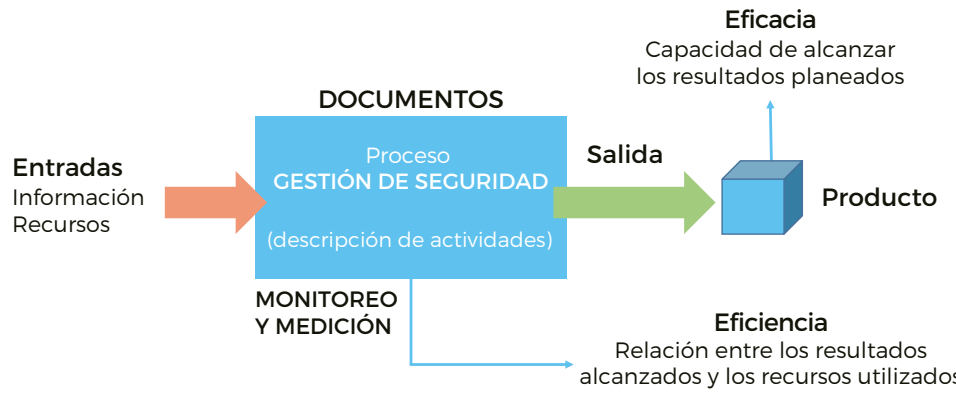
El mapa de procesos o la descripción de estos ayudan al empresario a graficar y conocer la manera en que los procesos interactúan; en esta construcción, igualmente, se busca detallar las actividades y tareas que cada proceso debe realizar para lograr el objetivo organizacional.

En la siguiente gráfica se visualiza la estructura de procesos de una organización (tomado del libro *Gestión por procesos*, de Icontec).



Dentro de las actividades diarias de una organización, y tomando como base los riesgos a los cuales están expuestas, se requiere "gestionar la seguridad". Esto implica la definición de actividades de control para la prevención y mitigación de riesgos, así como la identificación de potenciales pérdidas y la forma de abordarlas en caso de que se materialicen.

Una forma de gestionar la seguridad consiste en elaborar un proceso; la siguiente gráfica indica los elementos de este, dado que uno de sus objetivos es "gestionar los riesgos" que hacen parte de la organización.



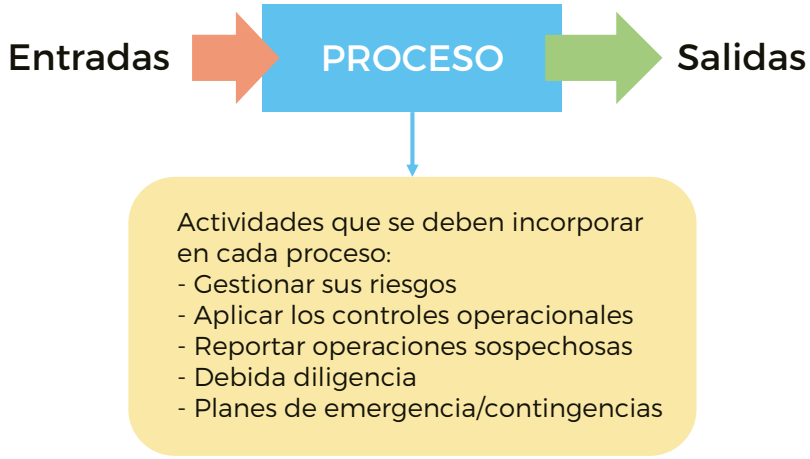
La norma ISO 31000 presenta las directrices para la gestión de riesgos, las cuales se describen en el siguiente marco de referencia (tomado de la norma ISO 31000:2018).

El "liderazgo y compromiso" nos indica que la gestión de riesgos debe estar integrada en todas las actividades de la organización y apoyada con un liderazgo y compromiso por parte de la alta dirección.

De ahí que todos los procesos que conforman la formación deben incorporar elementos que les permitan gestionar los riesgos; una forma de lograrlo es incorporar objetivos relacionados con la seguridad; por ejemplo:

Proceso	Objetivo convencional	Objetivo con enfoque de seguridad
Comercial	Captar clientes y cumplir las metas de las ventas.	Selección y administración de clientes confiables.
Compras	Adquirir bienes y/o servicios de calidad y buen precio.	Selección y administración de proveedores confiables.
Recursos humanos	Vincular personal idóneo y calificado.	Administrar el recurso humano confiable.
Financiero	Administración eficiente de los recursos.	Administración segura de los recursos, conocimiento del origen.
Manufactura	Elaborar los productos con base en los requerimientos del cliente.	Integridad en los productos; no contaminación con elementos ilícitos,
Logística y distribución	Ubicar los productos en las condiciones y tiempo requeridos.	Seguridad e integridad en las operaciones, libre de actividades ilícitas.
Tecnología	Contar con la infraestructura y equipo que le permitan el manejo de información.	Seguridad en la información para mantener la confidencialidad, integridad y disponibilidad.

Al identificar objetivos relacionados con la seguridad, cada proceso debe incorporar actividades que permitan "gestionar la seguridad"; estas son:



Al momento de incorporar estas actividades, la organización debe determinar que hacen parte de las medidas de control, para que se lleven a cabo en el momento justo. Por ello, las medidas de control tienen las siguientes características:

Suficientes: se implementan en la cantidad necesaria para no afectar la dinámica empresarial.

Comprensibles: son claras, sencillas y fáciles de aplicar.

Oportunas: actúan cuando realmente se necesitan.

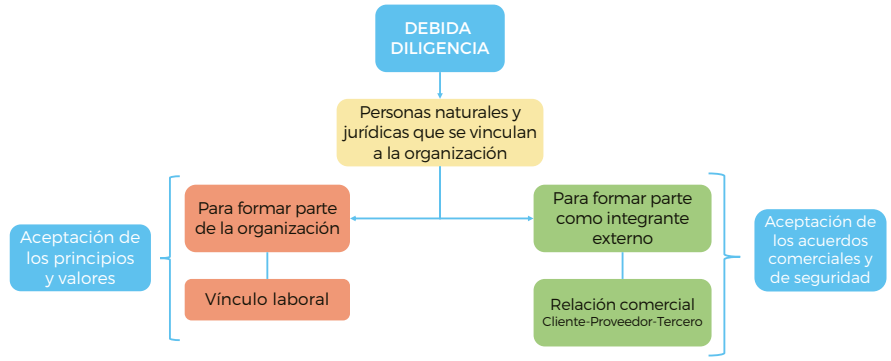
De igual forma, las "autoridades y responsabilidades" deben tener aspectos de seguridad, para determinar el "liderazgo y compromiso" en todos los niveles de la organización. A través de los manuales de funciones y perfiles del cargo, los colaboradores conocen sus responsabilidades en materia de seguridad.

Gestionando la seguridad para la debida diligencia ("due diligence")

De acuerdo con la ISO 37001:2016, gestión antisoborno, la debida diligencia se define como el "proceso para evaluar con mayor detalle la naturaleza y alcance del riesgo de soborno y para ayudar a las organizaciones a tomar decisiones en relación con operaciones, proyectos, actividades, socios de negocios y personal específicos".

Las actividades y procedimiento que soporta la debida diligencia son importantes para que la organización sea coherente con los principios y valores que promueve.

Por ejemplo, dentro de una organización la debida diligencia se lleva a cabo al momento de vincular o involucrar personas, clientes, proveedores, etc. En la siguiente gráfica se muestra su aplicación:



La “debida diligencia” debe ser a todos los cargos de la organización; a través de la inducción, reinducción, capacitaciones y otros mecanismos, la organización debe transmitir su importancia y aplicación en cada una de las actividades y toma de decisiones.

Gestión de la seguridad para los asociados de negocio en la cadena de suministros

Con base en los principios del Marco Normativo SAFE, expedido por la Organización Mundial de Aduanas (OMA), el cual busca asegurar y facilitar el comercio internacional, se establecieron los requerimientos mínimos de seguridad para que la relación comercial entre cliente y proveedor se enmarque en prácticas de prevención de riesgos.

En Colombia, el programa Operador Económico Autorizado (OEA), a través de la DIAN, emitió la Circular N.° 000006 del 16 de septiembre de 2016, para promover la aplicación de los criterios de seguridad para la prevención de actividades ilícitas en la cadena de suministro, tales como: lavado de activos, contrabando, tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, terrorismo, financiación del terrorismo, tráfico de armas y narcotráfico.

A continuación se relacionan los requisitos mínimos de seguridad aplicados, para que la organización elabore un “acuerdo de seguridad” o una “manifestación suscrita”, en donde el asociado de negocio se compromete a implementar y cumplir los siguientes criterios de seguridad:

- Asociados de negocio: realizando un conocimiento de los asociados de negocio a través de un proceso de selección seguro y confiable.
- Controles de acceso físico: estableciendo un control de acceso de colaboradores, visitantes y contratistas a las instalaciones para prevenir el acceso no autorizado.
- Seguridad del personal: contando con un proceso de selección y retiro de personal para asegurar la confiabilidad.
- Seguridad de los procesos: garantizando la integridad y seguridad en las actividades que hacen parte de la prestación del servicio.
- Seguridad física: implementando medidas que garanticen la seguridad de las instalaciones.
- Seguridad en tecnología de la información: contando con medidas que protejan el acceso no autorizado a la información, documentación y sistemas de información para mantener la confidencialidad en la prestación del servicio y sus operaciones.

- Entrenamiento en seguridad y conciencia de amenazas. Estableciendo actividades de capacitación y formación enfocadas a desarrollar la seguridad e integridad de sus operaciones.

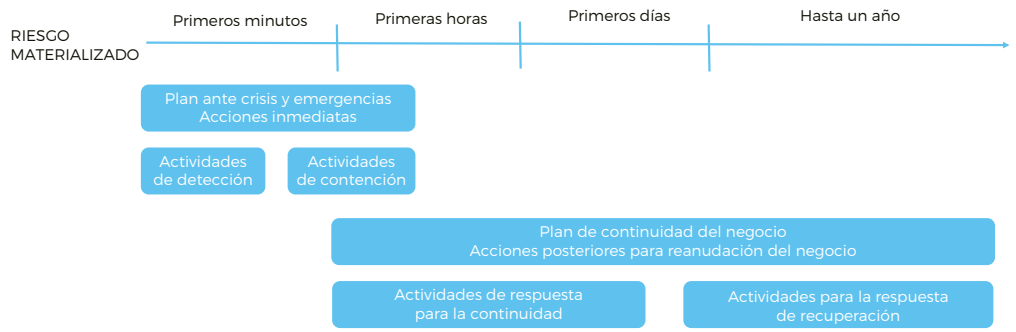
A través de visitas o auditorías de segunda parte a los asociados de negocio, se valida el cumplimiento de estos requisitos, con base en el nivel de riesgos o criticidad.

Gestión de la seguridad para continuar con las actividades del negocio frente a un riesgo materializado

Frente a un evento o riesgo materializado, la organización necesita dar respuesta de manera oportuna y efectiva para proteger su imagen; esto implica tomar acciones para que el impacto del evento no afecte la continuidad y normal funcionamiento de sus operaciones.

En ocasiones, el impacto se puede manejar dentro de los procesos de la organización. Sin embargo, cuando la escala del evento sobrepasa considerablemente la capacidad de la organización, entonces es necesario un enfoque sistemático para la gestión del incidente crítico.

En la siguiente gráfica se describen las acciones en caso de la materialización de un riesgo:



La continuidad del negocio proporciona a la organización la capacidad para seguir operando con sostenibilidad ante una interrupción significativa; aborda la exposición al riesgo de interrupción de una manera oportuna.

Igualmente, proporciona elementos claves para que la organización sostenga un buen gobierno corporativo, mantenga su participación en el mercado, así como la cartera de sus clientes y confianza a las partes interesadas.

6.2. Cuarta revolución industrial y su impacto en la seguridad de la cadena de suministro

Por: Reinaldo Andrés Rodríguez Guerrero Director General Grupo OET

El Foro Económico Mundial define la cuarta revolución industrial como "la combinación de sistemas digitales, físicos y biológicos en pro de la transformación de la humanidad" (Acevedo Vélez, 2018). Es una tendencia irreversible que está afectando cada aspecto de nuestras vidas y frente a la cual la seguridad de la cadena de suministro no es ajena.

Unas de las características distintivas de la cuarta revolución industrial es el uso de tecnologías digitales, como el Big Data, la realidad virtual, el Internet de las Cosas (IoT, por su sigla en inglés), la inteligencia artificial, el uso de robots y drones, entre otras, las cuales representan oportunidades muy valiosas para la seguridad de la cadena de suministro, pero, así mismo, implican riesgos que deben ser considerados y mitigados desde el momento de su implementación, de forma tal que los beneficios obtenidos sean mayores que los riesgos de su adopción.

Oportunidades

Una de las tecnologías digitales de mayor uso hoy en día en la cadena de suministros es la Internet de las Cosas o IoT, mediante una de sus principales aplicaciones en dispositivos AVL (Automatic Vehicle Location) o más conocidos como GPS o dispositivos satelitales. Son innumerables los beneficios, tanto en productividad, como en eficiencia y seguridad, que aporta esta tecnología para la cadena de suministro. En materia de seguridad, estas tecnologías permiten identificar en tiempo real la ubicación de buques, aviones o vehículos y la carga, planear e identificar rutas seguras y generar acciones de reacción en caso de novedades presentadas durante la operación de transporte.

Tecnologías como AVL generan miles de datos diarios, que a su vez pueden ser aprovechados a través de otras de las tecnologías bandera de la cuarta revolución digital: la Big Data. Mediante esta, la minería de datos y la analítica de datos se puede obtener información valiosa para la seguridad en la cadena de suministros, como la identificación de puntos de almacenamiento y rutas seguras, vehículos, conductores y proveedores de servicios logísticos confiables, cargas más susceptibles a robo o saqueo, entre otros.

Pero los procesos anteriores no serán posibles sin la tecnología de la nube, la cual se refiere al acceso a información a través de internet, desde cualquier lugar, mediante una computadora o un celular. El acceso a información en

tiempo real permite tomar decisiones y acciones de forma oportuna, tanto de manera preventiva como correctiva.

Riesgos

Si bien son muchos los beneficios que generan tecnologías como el AVL o GPS, estas no están exentas de riesgos. Recientemente se informó sobre diversos ataques de suplantación a sistemas GPS (Goward, 2017), y el Departamento de Seguridad Nacional de los Estados Unidos ha emitido circulares informativas con recomendaciones para la mitigación de riesgos relacionados con vulnerabilidad de los sistemas GPS (U.S. Department of Homeland Security, 2019), debido a que las señales basadas en el espacio del GPS son de baja potencia y no están encriptadas, lo que las hace susceptibles a interrupciones intencionales y no intencionales. A pesar de lo anterior, los beneficios que trae esta tecnología son inmensos, por lo que la recomendación para la mitigación de estos riesgos pasan por la verificación de contar con proveedores de sistemas AVL confiables y con alternativas de respaldo frente a posibles fallas que puedan presentar dichos sistemas en operaciones donde la seguridad sea un aspecto crítico.

Otro de los riesgos que se deben considerar es la seguridad en el acceso a la información. Existe un amplio debate sobre si es más seguro almacenar la información en la nube o en servidores propios. Lo cierto es que existe una tendencia cada vez mayor a almacenar información en la nube (si su compañía usa tecnología AVL seguramente ya lo está haciendo, o si utiliza proveedores de correo, como Office 360 o Gmail). Acá de nuevo es clave contar con asociados de negocio digitales que tengan implementadas prácticas seguras para el manejo de la información, establecer políticas para la seguridad de la información y crear conciencia sobre las buenas prácticas en seguridad por parte de los usuarios de las soluciones digitales.

Algunas recomendaciones

- La implementación de tecnologías digitales disruptivas debe estar alineada con la planeación estratégica de la empresa.
- La empresa debe definir una política de seguridad de la información, alineada con las políticas de seguridad de sus sistemas integrados de gestión.
- Las matrices de riesgos deben considerar los activos de información de la compañía, incluyendo sus activos digitales (bases de datos, aplicaciones, interfaces, robots, drones), las vulnerabilidades y planes de contingencia, para minimizar los riesgos por los cuales se pueden ver afectadas.
- La creación de conciencia sobre los riesgos de las tecnologías digitales debe ser permanente y constante dentro de las compañías, e involucrar a todos los asociados de negocio que componen la cadena de suministros.
- Los proveedores de soluciones digitales (sean estas AVL, aplicaciones web, servicios en la nube) son asociados de negocios cada vez más críticos, y deberían alinear sus políticas de seguridad de la información con las de toda la cadena.

- El involucramiento del equipo humano en la implementación de nuevas tecnologías digitales es clave. Ninguna tecnología puede reemplazar totalmente el criterio humano en la toma de decisiones de seguridad. Involucre al equipo humano en estos procesos, y los resultados serán mucho más exitosos.

Referencias

Acevedo Vélez, M. (1 de agosto de 2018). *¿Qué es la Cuarta Revolución Industrial?* Obtenido de la Pontificia Universidad Bolivariana: https://www.upb.edu.co/es/noticias/que-es-la-cuarta-revolucion

Goward, D. (8 de agosto de 2017). *Spoofing attack reveals GPS vulnerability.* Obtenido de GPS World: https://www.gpsworld.com/expert-opinion-spoofing-attack-reveals-gps-vulnerability/

U.S. Department of Homeland Security (13 de marzo de 2019). *Global Positioning System (GPS) Vulnerabilities for Critical Infrastructure Fact Sheet.* Obtenido de Official Website of the Department of Homeland Security: https://www.dhs.gov/publication/gps-vulnerabilities-critical-infrastructure-fact-sheet

CAPÍTULO 7

SIPLAFT y SARLAFT

7. SIPLAFT y SARLAFT
Definición, amenazas, riesgos, antecedentes y soportes normativos, guías para la adopción de sistemas

Por: Carlos Alfonso Boshell Norman
Subgerente Implementación Sistema de Administración Riesgos LA/FT
Superintendencia y Sector de la Vigilancia y Seguridad Privada

En la actualidad, el lavado de activos y la financiación del terrorismo se han convertido en una verdadera amenaza global ante el crecimiento de la delincuencia organizada, que conlleva el manejo de recursos incalculables, cuya procedencia es incierta y difícil de detectar. El lavado de activos se realiza con el objeto de encubrir la actividad criminal con la cual está relacionado. Como resultado de esta rápida evolución, la lucha contra estos delitos se ha convertido en una prioridad para los gobiernos, los organismos reguladores y los organismos internacionales, en vista de que este hecho supone un riesgo muy importante para los países en los que los lavadores operan.

Definición

¿Qué es el lavado de activos?

Es la modalidad mediante la cual organizaciones criminales buscan dar apariencia de legalidad a los recursos que obtienen de sus actividades ilícitas, mediante la incorporación de estos en el circuito económico legal. A través de esta actividad, las bandas delincuenciales consiguen hacer uso de estos activos, sin poner en peligro su reinversión en nuevas actividades ilícitas o lícitas. Para el caso colombiano, el lavado de activos está tipificado como una actividad delictiva, descrita en el artículo 323 del Código Penal, así: "el que adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades de tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias psicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito, incurrirá, por esa sola conducta, en prisión

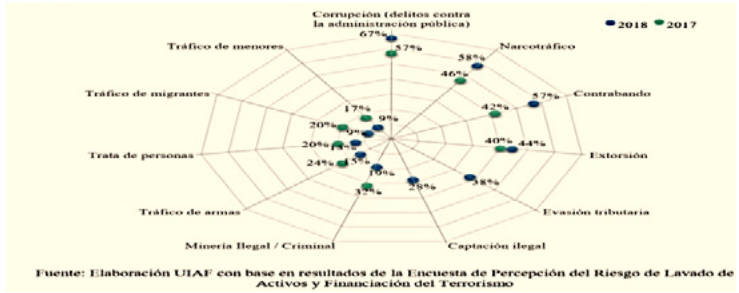
de 10 a 30 años y multa de 650 a 50.000 salarios mínimos legales mensuales vigentes", que en la actualidad cuenta con 65 delitos fuente.

¿Qué es la financiación del terrorismo?

Es el apoyo financiero, en cualquier forma, al terrorismo o a aquellos que lo fomentan, planifican o están implicados en él. Se debe tener en cuenta que es complicado definir el terrorismo en sí mismo, porque el término puede tener connotaciones políticas, religiosas y nacionales, dependiendo de cada país. El lavado de activos y la financiación del terrorismo, por lo general, presentan características de operaciones similares, sobre todo con relación al ocultamiento, pero aquellos que financian el terrorismo transfieren fondos que pueden tener un origen legal o ilícito, encubriendo su fuente y destino final. Para el caso colombiano, el artículo 345 del Código Penal dice: "el que 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 de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas, incurrirá en prisión de trece (13) a veintidós (22) años y multa de mil trescientos (1.300) a quince mil (15.000) salarios mínimos legales mensuales vigentes".

Amenazas

La amenaza se entiende como la identificación de las actividades ilícitas que dan origen a los recursos ilegales que son lavados. En la gráfica 1 se presenta la proporción de encuestados, a nivel nacional, que consideran que las actividades ilícitas enunciadas representan una de las principales amenazas. Las cinco principales actividades ilícitas que los encuestados destacan como la mayor amenaza son: la corrupción, con un 67%, seguida por el narcotráfico, con un 58%; al contrabando le corresponde el tercer lugar, con 57%, seguido por la extorsión, con 44%, y la evasión tributaria, con 38%.

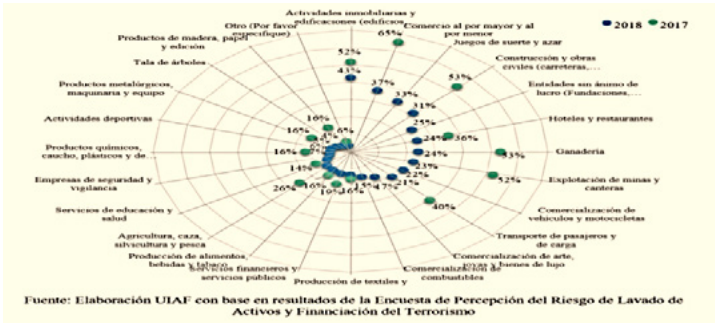


Fuente: Elaboración UIAF con base en resultados de la Encuesta de Percepción del Riesgo de Lavado de Activos y Financiación del Terrorismo

LAVADO DE ACTIVOS	FINANCIACIÓN DEL TERRORISMO
Siempre se va a dar respecto de dineros o activos que provengan de actividades ilícitas representadas en los delitos subyacentes o fuente.	Se puede dar con dineros, activos o apoyo logístico proveniente de actividades lícitas o ilícitas.
El único interés por parte de la organización criminal es legalizar sus ganancias.	Los fines son el sostenimiento de la organización terrorista.
Los montos en las transacciones son grandes y a menudo estructurados para evitar la obligación de reportar.	Los montos transaccionales son pequeños, generalmente por debajo de los montos sujetos a reporte.
Las organizaciones criminales operan normalmente a través de una red compleja de transacciones que a menudo involucra compañías pantalla o de papel.	No existe un perfil financiero que se aplique a los terroristas operativos.
Normalmente el dinero regresa a la organización que comete el ilícito, es decir, tiene una trazabilidad circular.	El dinero generado es utilizado para difundir actividades y grupos terroristas, es decir, tiene una trazabilidad lineal.

Vulnerabilidades

Se entienden como las situaciones o hechos que pueden ser aprovechados o utilizados para que las amenazas se materialicen. En la gráfica 2 se presenta la proporción de encuestados a nivel nacional que consideran que las actividades económicas enunciadas son las más vulnerables para lavar activos. Las cinco principales que los encuestados perciben como vulnerables son: actividades inmobiliarias y edificaciones (43%), comercio al por mayor y al por menor (37%), juegos de suerte y azar (33%), construcción y obras civiles (31%) y entidades sin ánimo de lucro (25%).



Fuente: Elaboración UIAF con base en resultados de la Encuesta de Percepción del Riesgo de Lavado de Activos y Financiación del Terrorismo

Antecedentes y soportes normativos ALA/CFT

Corría el segundo lustro del siglo anterior, cuando las mafias estadounidenses se veían en la necesidad de ocultar el producto de actividades delictivas fruto del tráfico de armas, alcohol, juego clandestino, extorsión, prostitución, entre otras, y fue a través de redes de "lavanderías industriales para ropa" y "lavaderos para autos" como pretendían presentarlos como ganancias de origen legal; se cree que de esta situación viene el concepto de "lavado de dinero".

Ante la creciente demanda y por tráfico ilícito de estupefacientes, en la Organización de las Naciones Unidas (ONU) en Nueva York, corriendo el 30 de marzo de 1961, se aprobó la "Convención Única sobre Estupefacientes", enmendada posteriormente por el Protocolo de Modificaciones hecho en Ginebra (Suiza) el 25 de marzo de 1972, que buscaba combatir el lavado de activos y otras amenazas contra el sector financiero especialmente, y en el año 1975 el G-10 establece el Comité de Supervisión Bancaria de Basilea (1974), a fin de fortalecer la solidez de los sistemas financieros. Colombia ratifica dicha convención y protocolo con la promulgación de la Ley 13 de 1974.

Las altas sumas generadas por el tráfico de drogas fueron depositadas en los bancos sin ningún tipo de control. El lavado de activos fue advertido como manifestación jurídica en los países desarrollados, y es así como en 1988 la ONU aprueba la "Convención contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas", en la Convención de Viena; en ese mismo año se promulga la "Declaración de Principios", que fue una de las formulaciones que realizó el Comité de Basilea para la reglamentación bancaria y las prácticas de vigilancia. Los paises integrantes del G-7 conforman en 1989 el Grupo de Acción Financiera Internacional (GAFI/FATF), y en esta línea, el GAFI publicó en 1990 las 40 Recomendaciones, que son reconocidas hoy en día como el estándar que deben cumplir los países cooperantes para encarar formalmente el Lavado de Activos (LA).

Colombia, con la voluntad política y el apoyo de los gremios del sector financiero, fue receptiva de los estándares internacionales mencionados, iniciando un largo recorrido en la implementación de instrumentos, mecanismos y estándares de lucha contra el LA. En este sentido, y con el fin de cumplir con los principios de Basilea, se interviene la actividad de las instituciones vigiladas por las Superintendencias Bancaria y de Valores (hoy Superintendencia Financiera de Colombia) con el Decreto 1872 de 1992. Asimismo, a través del Decreto 663 de 1993, el Gobierno Nacional instaura las primeras medidas administrativas tendientes a que el sector financiero previniera el lavado y colaborara con las autoridades competentes; tal antecedente daría origen a lo que fue denominado como Sistema Integral de Prevención de Lavado de Activos (SIPLA), el cual evolucionó tiempo después a un Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo (SARLAFT). Durante este mismo año fue ratificada la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas, mediante la Ley 67/1993.

Corría el año 1995 cuando surgen las Unidades de Inteligencia Financiera (UIF), dada la necesidad de contar con organismos capaces de centralizar, procesar, analizar y divulgar a las autoridades de investigación y judicialización la información financiera requerida para combatir el delito de LA. Además, se crea el Grupo Egmont, instancia que reúne a todas las UIF del mundo; al día de hoy existen 159 UIF alrededor del planeta. Ese mismo año entra en ejecución la Ley 190/95, que viene a ser el primer marco normativo para combatir la corrupción. Impone a las Superintendencias Bancaria y de Valores que las obligaciones

de los artículos 102 al 107 del Estatuto Orgánico del Sistema Financiero (EOSF) asignaran a una de sus dependencias la función de control de operaciones de LA, y también impuso a dichas superintendencias entregar un informe anual a la Fiscalía General de la Nación (FGN), en el que dieran cuenta de la labor de detección realizada.

Paralelamente se aprueba el Decreto 950/95, que crea la Comisión de Coordinación Interinstitucional para el Control del Lavado de Activos (CCICLA), como organismo consultivo del Gobierno Nacional y ente coordinador de las acciones que desarrolla el Estado colombiano para combatir el lavado de activos. Al año siguiente, la Organización de los Estados Americanos (OEA) se pronuncia respecto a la corrupción, y reconoce expresamente su trascendencia internacional y la necesidad de contar con un instrumento que promueva y facilite la cooperación entre los países para enfrentarla. Por tal razón, en marzo de 1996 los Estados miembros adoptan la Convención Interamericana contra la Corrupción, la cual se convierte en el primer instrumento jurídico en su tipo para hacerle frente a dicho fenómeno; adicionalmente, en el orden nacional se promulga la primera ley de extinción del derecho de dominio sobre los bienes adquiridos en forma ilícita (Ley 333 de 1996), y así el país es pionero en el mundo en su regulación, y en la actualidad se encuentra establecida en el Código de Extinción de Dominio. Colombia se adhiere a la Convención Interamericana contra la Corrupción, ante la aprobación de la Ley 412 de 1997.

Mediante la Ley 365 de febrero 21 de 1997, por la cual se establecen normas tendientes a combatir la delincuencia organizada y se dictan otras disposiciones, se tipifica penalmente el LA en el país a partir de la división conveniente del delito de receptación, con el propósito de buscar una mayor pena al nuevo delito, que admitiría de manera expresa el concurso con un delito subyacente (como extorsión, enriquecimiento ilícito, narcotráfico, secuestro extorsivo, etc.), y para cerrar ese mismo año la ONU aprueba el Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas.

Con el fin de detectar, prevenir y en general luchar contra el LA en todas las actividades económicas, se crea la Unidad Administrativa Especial de Información y Análisis Financiero por medio de la Ley 526 de 1999, como la Unidad de Inteligencia Financiera del país. Para cumplir con su objetivo, la UIAF centraliza, sistematiza y analiza la información recaudada, en desarrollo de lo enunciado en los artículos 102 a 107 del EOSF. Asimismo, la UIAF ejerce el papel de Secretaría Técnica de la CCICLA.

La ONU aprueba el Convenio Internacional para la Represión de la Financiación del Terrorismo (1999) y la Convención de Palermo contra la Delincuencia Organizada Transnacional (2000), y finalizando ese mismo año se crea formalmente el Grupo de Acción Financiera de Sudamérica (GAFISUD), en la actualidad GAFILAT (Grupo de Acción Financiera de Latinoamerica), mediante el memorando de entendimiento constitutivo del grupo suscrito por los gobiernos de nueve países: Argentina, Bolivia, Brasil, Chile, Colombia, Ecuador, Paraguay, Perú y Uruguay. Esta organización intergubernamental

regional busca prevenir y combatir el LA/FT/FPADM, a través del compromiso de mejora continua de las políticas nacionales en dichos temas, y por último la Convención contra la Corrupción (2003). En Colombia, estos instrumentos fueron ratificados, en su orden, por medio de las Leyes 804/808/800 de 2003 y la Ley 970 de 2005. Los atentados a las Torres Gemelas también dieron origen a que se adoptara, en el marco de la OEA, la Convención Interamericana contra el Terrorismo (2002), con lo cual la comunidad interamericana dio un paso importante en su estrategia colectiva para combatir este flagelo. En Colombia, dicha convención fue aprobada mediante la Ley 1108 de 2006. Con la Ley 1186/08, Colombia ratifica el memorando de entendimiento constitutivo del GAFISUD (hoy GAFILAT). Con la Ley 1266/08 se promulga la ley de habeas data, con la cual se dictaron disposiciones generales en la materia y se reguló el manejo de bases de datos personales relacionadas específicamente con información de naturaleza financiera, crediticia, comercial, de servicios y la proveniente de terceros países, y con la Ley 1231/08, las empresas de *factoring* quedaron obligadas a informar a la UIAF sobre cualquier operación sospechosa de LA o actividad delictiva. A raíz de los atentados terroristas del 11 de septiembre del 2001, en Estados Unidos, el GAFI publicó nueve (9) recomendaciones especiales contra la FT (actualmente unificadas con las 40 recomendaciones). Para dar cumplimiento a la Recomendación Especial II, hoy recogida como estándar 5, se tipificó el delito de FT en el país, por medio de la Ley 1121 de 2006. El tipo penal descrito en esta ley no solo incluye aquellas conductas detalladas en el Convenio Internacional de las Naciones Unidas para la Represión de la Financiación del Terrorismo (1999), sino que abarca, además, todas las posibles actividades de terrorismo y de los grupos terroristas, o de los grupos armados al margen de la ley. Asimismo, con la aprobación de la Ley 1121, se le asignaron a la UIAF competencias en prevención y detección del delito de FT.

El Gobierno Nacional desarrolló una estrategia para combatir los principales focos de corrupción del país. Esta normatividad quedó plasmada en el nuevo Estatuto Anticorrupción, con la expedición de la Ley 1474 de 2011, las normas que siguen vigentes del primer estatuto (Ley 190/95) y las convenciones internacionales adoptadas por Colombia sobre la materia. Cabe mencionar que el nuevo Estatuto Anticorrupción retoma la figura de la Comisión Nacional de Moralización como una instancia integrada por los superiores de las ramas del poder público y los organismos de control. A la vez, se crea la Secretaría de Transparencia por el Decreto 4637 de 2011.

Más adelante, la obligatoriedad de reportar recae sobre los clubes deportivos, a través de la Ley 1445 de 2011. De igual manera, la Ley 1508 de 2012 –que establece el régimen jurídico de las Asociaciones Público-Privadas (APP)– exigió a las fiduciarias reportar a la UIAF el nombre del fideicomitente, del beneficiario, el valor de los recursos administrados a través del patrimonio autónomo constituido por el contratista y la demás información sobre proyectos de las APP que la UIAF requiera.

En el año 2012, el Congreso expidió la Ley Estatutaria 1581, que establece el régimen general aplicable en materia de protección de datos personales en el

país –Ley de habeas data–, cuyo objeto fue desarrollar el derecho constitucional de todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos. En este sentido, la facultad por ley concedida a la UIAF para levantar la reserva bancaria, tributaria, cambiaria y bursátil, entre otras, sin vulnerar el derecho constitucional al habeas data, se justifica por el perjuicio que los delitos de LA/FT causan a la economía y seguridad pública, lo cual amerita la estricta reserva que la Unidad debe mantener sobre su información.

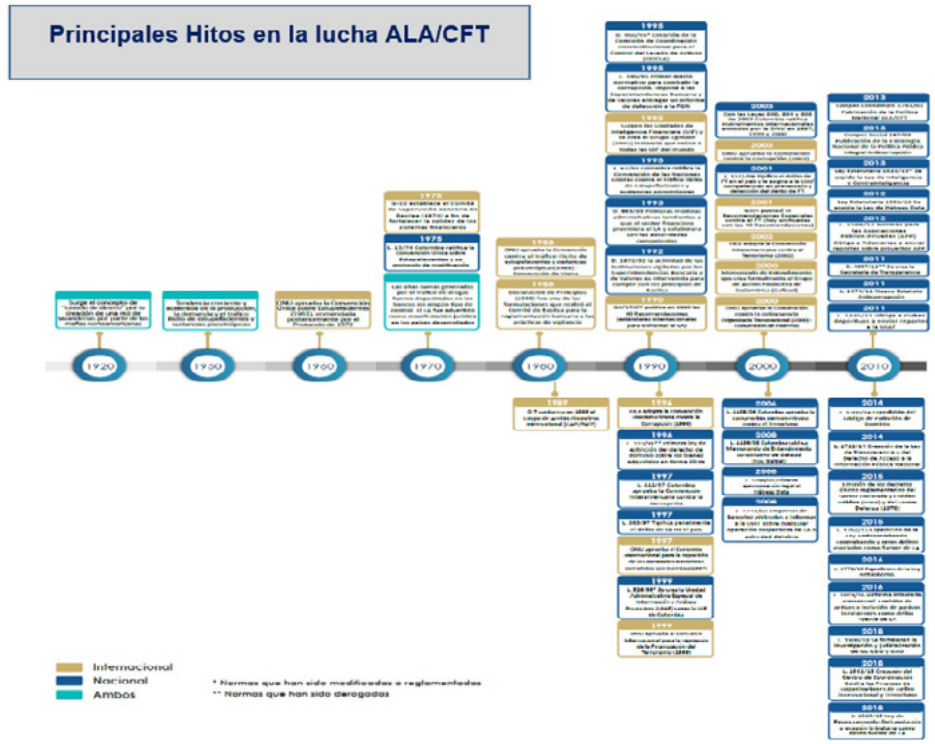
Durante el periodo 2013-2016 también se registraron hechos destacados para el desarrollo del Sistema ALA/CFT en el ámbito nacional:

- Expedición de la Ley Estatutaria 1621, que define a la UIAF expresamente como un organismo de inteligencia del Estado colombiano con asiento en la Junta de Inteligencia Conjunta, por lo que su misionalidad se enmarca en los requerimientos anuales formulados por el Presidente de la República en el Plan Nacional de Inteligencia;
- Publicación de la Política Nacional ALA/CFT, consignada en el documento del Consejo Superior de Política Económica y Social, Conpes Económico 3793, la cual avanzó en paralelo con el Enfoque Basado en Riesgo que termina con la difusión de la primera Evaluación Nacional de Riesgo de LA/FT del país;
- Presentación de la Estrategia Nacional de la Política Pública Integral Anticorrupción, con el propósito de fortalecer las herramientas y mecanismos para la prevención, investigación y sanción de la corrupción (documento Conpes Social 167);
- Expedición del Código de Extinción de Dominio por medio de la Ley 1708 de 2014;
- Creación de la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional (Ley 1712/2014);
- Emisión en el 2015 de los decretos únicos reglamentarios del Sector Hacienda y Crédito Público (Decreto 1068) y del Sector Defensa (Decreto 1070);
- Incorporación de instrumentos para prevenir, controlar y sancionar el contrabando, actividad delictiva que pasa a ser delito fuente de LA (Ley Anticontrabando 1762 de 2015);
- Publicación de la Ley Antisoborno, donde se destaca, entre varios temas, la lucha contra la corrupción transnacional al establecer responsabilidad sobre personas jurídicas (Ley 1778 de 2016);
- Adopción de una reforma tributaria estructural (Ley 1819 de 2016) que fortaleció los mecanismos para la lucha contra la evasión y la elusión fiscal, además de incluir la omisión de activos o inclusión de pasivos inexistentes como delito fuente de LA.

A mediados del 2018 se fortalecen la investigación y judicialización de los Grupos Delictivos Organizados (GDO) y los Grupos Armados Organizados (GAO), mediante la Ley 1908. Por otro lado, se creó recientemente el Centro de Coordinación Contra las Finanzas de Organizaciones de Delito Transnacional

y Terrorismo, por medio de la Ley 1941 de 2018. La nueva instancia tiene como objetivo perseguir y desmantelar las redes de dinero y bienes de origen ilícito o empleados en actividades ilícitas. La Secretaría Técnica del Centro es ejercida por la UIAF, a fin de generar sinergia y sincronización tanto estratégica como de ejecución entre la Fuerza Pública, los organismos de inteligencia y contrainteligencia, la FGN y las autoridades judiciales.

Expedida también en diciembre del 2018, la Ley de Financiamiento (Ley 1943) estableció un nuevo delito fuente de LA: defraudación o evasión tributaria. Con este delito no solo se pretende prevenir su comisión, sino sancionar de forma eficaz a los defraudadores de las arcas del Estado, quienes mediante maniobras fraudulentas requieren a la autoridad tributaria para que efectúe reembolsos y devoluciones de dinero de impuestos por concepto de saldos a favor.



Sistemas contra el lavado de activos y financiación del terrorismo

Normativamente y las buenas prácticas en prevención nos han llevado a diseñar, implementar y desarrollar los siguientes:

- **SIPLA:** Sistema para la Prevención y control del Lavado de Activos
- **SARLAFT:** Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo

- **SIPLAFT:** Sistema Integral de Prevención y control del Lavado de Activos y Financiación del Terrorismo.
- **SAGRLAFT:** Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo

El **SIPLAFT** debe cumplir, como mínimo, en:

- Diseño del sistema
- Aprobación del sistema
- Constancia de la aprobación de las políticas
- Comunicación de la politica, objetivo
- Nombramiento del funcionario de cumplimiento
- Capacitación sobre LA/FT
- Documentación del sistema

El **SARLAFT** debe cumplir con las etapas consistentes en:

- Identificar riesgos de LA/FT
- Medir los riesgos de LA/FT
- Controlar los riesgos de LA/FT
- Monitoreo de los riesgos de LA/FT

El **SARLAFT** debe cumplir con los elementos que soportan este propósito, que son:

- Políticas
- Procedimientos
- Documentación
- Estructura organizacional
- Órganos de control
- Infraestructura tecnológica
- Divulgación de la información
- Capacitación

Guía para la adopción de un sistema de gestión de riesgo

La gestión de riesgo es una parte integral de las buenas prácticas de administración y un elemento esencial de la buena dirección corporativa. Por ello, se dice que la administración del riesgo forma parte del Buen Gobierno Corporativo y de la Responsabilidad Social Empresarial.

Para la elaboración de un sistema de gestión del riesgo de lavado de activos y de financiación del terrorismo, se sugiere tomar en consideración las siguientes disposiciones y estándares internacionales:

ETAPA UNO. Diagnóstico

Paso 1. Comprometer a los dueños y directivos del negocio.
Paso 2. Determinar el contexto externo e interno en el que se desenvuelve la empresa.
Paso 3. Determinar los factores de riesgo de LA/FT.
Paso 4. Elaboración del diagnóstico del riesgo de LA/FT.
Paso 5. Definición de las metodologías y herramientas para la gestión de riesgos de LA/FT.

ETAPA DOS. Identificación de los riesgos

Paso 1. Identificar los eventos de riesgo para cada factor de riesgo y sus causas.

ETAPA TRES. Medición o evaluación de los riesgos

Paso 1. Determinar los criterios para la medición de los riesgos.

ETAPA CUATRO. Adopción de controles-medidas preventivas. Calificación y valoración de los controles de los riesgos de LA/FT

1. Tipos de controles
2. Formas de los controles
3. Clasificación de los controles sobre su implementación
4. Valoración de los controles

Opciones de tratamiento-determinación de controles

Paso 1. Definir los controles para mitigar cada uno de los eventos de riesgo.
Paso 2. Definir los procedimientos para la aplicación de los controles.
Paso 3. Diseñar y aplicar un plan de tratamiento de los riesgos de LA/FT.
Paso 4. Seguimiento y control de las operaciones de las contrapartes, para efectos de la detección y reporte de operaciones a las autoridades.

ETAPA CINCO. Divulgación y documentación (capacitación y consulta)

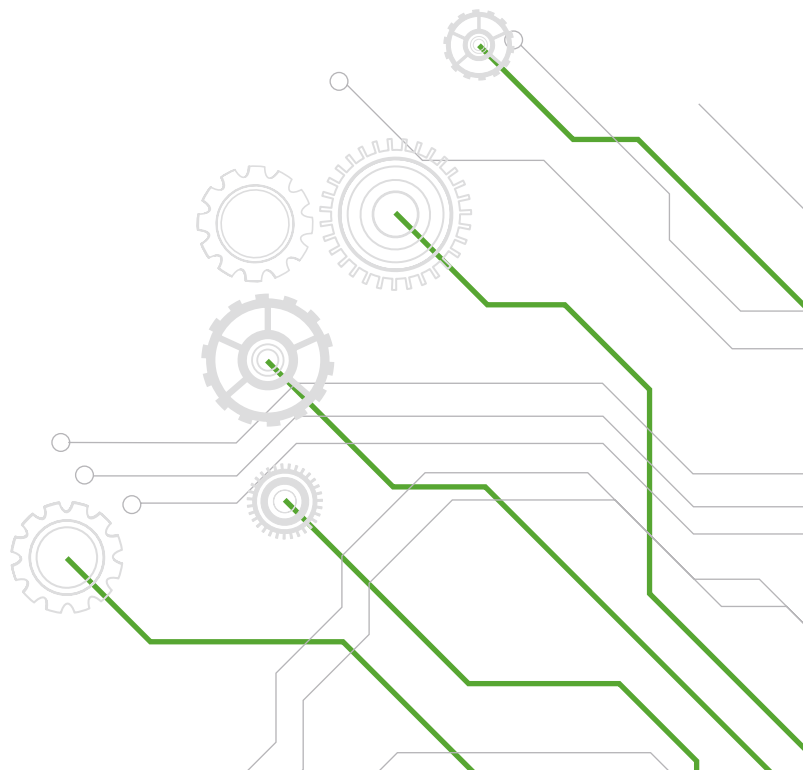
Paso 1. Proveer un sistema de documentos y registros de las etapas y elementos del Sistema de Gestión del Riesgo de LA/FT.
Paso 2. Definir procedimientos para la realización de reportes internos y externos.
Paso 3. Diseñar y ejecutar el programa de capacitación y del plan de divulgación del Sistema de Gestión del Riesgo de LA/FT.
Paso 4. Divulgar los controles para mitigar el riesgo de LA/FT.
Paso 5. Definir procedimientos para la imposición de sanciones ante el incumplimiento de la aplicación de controles.

ETAPA SEIS. Seguimiento o monitoreo

Paso 1. Definir procedimientos para la realización de actividades de monitoreo o seguimiento del Sistema de Gestión del Riesgo de LA/FT.

CAPÍTULO 8

BUENAS PRACTICAS



8.1. La norma ISO 28000, sistema de gestión de seguridad en la cadena de suministro, aplicada al contexto policial

Por: Eduardo Hernández Ruiz, José Ángel Vidaña Meraz y Rosa María del Carmen Jiménez Mendoza, del Consejo de Seguridad en Cadena de Suministro, México; Benjamín Grajeda Regalado y José Luis Vilchis Maya, de la Gendarmería Nacional de México.

¿Qué es la ISO 28000?

Actualmente existe una mayor demanda de normas y mejores prácticas para prevenir y mitigar las amenazas a las que están expuestas las organizaciones de todo el mundo. Estas organizaciones están implementando sistemas de gestión de riesgos en todos los eslabones de su cadena de suministro, para desarrollar procesos integrales y sistemáticos de prevención, protección, preparación, mitigación, respuesta, continuidad y restablecimiento en sus operaciones. La norma internacional ISO 28000 es un Sistema de Gestión de la Seguridad en la Cadena de Suministro, que permite identificar la vulnerabilidad en procesos críticos en cada eslabón de su cadena logística y suministro, mediante el desarrollo de controles preventivos, conocidos como contramedidas.

Esta norma internacional tiene aplicación en el sector privado, organismos no gubernamentales y un sector poco conocido, el público, concretamente en el ámbito policial.

El estándar ISO 28000 aplicado al contexto policial en la protección de ciclos productivos

Ante los índices delictivos que se presentan en México, en el año 2014 se creó un grupo especializado dentro de la Policía Federal Mexicana, con el nombre de Gendarmería Nacional, nombrando como titular al Ing. Benjamín Grajeda Regalado, con capacidades de planeación y coordinación en conjunto con los tres órdenes de gobierno (Federación, Estados y Municipios), con el objetivo de proteger todos los eslabones de la cadena de suministro, a los cuales en lo sucesivo nos referiremos como ciclos productivos.

¿Por qué implementar la ISO 28000 en un contexto policial?

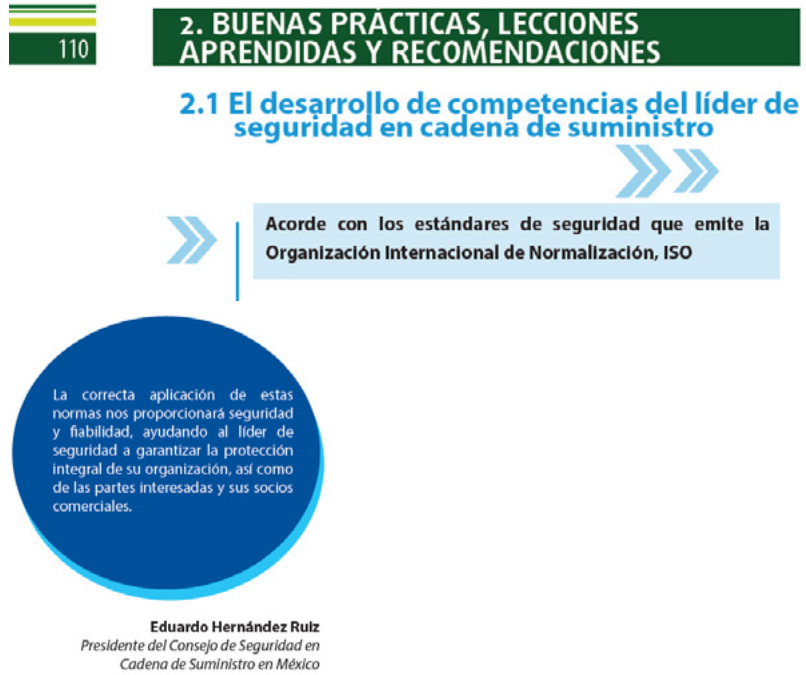
La norma ISO 28000 fue creada por la Organización Internacional de Normalización (ISO) en el año 2007, concebida sobre todo (mas no limitada) para organizaciones con actividades prioritariamente logísticas; sin embargo, México fue el primero en adoptar esta norma, para aplicarla en un contexto

policial a partir del año 2016, lo cual dio como resultado la creación de un proyecto académico especializado para la División de Ciclos Productivos de la División de la Gendarmería Nacional, en la Policía Federal de México, a partir del año 2018, denominado "Diplomado de Protección a Ciclos Productivos", con una duración total de 140 horas.

Antecedentes y línea de tiempo

2016

En el año 2016, la Jefe del Área de Asistencia y Cooperación para la Investigación Judicial y Frente de Seguridad Empresarial, Mayor Gelga Buitrago Martínez (DIJIN FSE) me invitó a colaborar en la V edición de la *Guía de Seguridad para los actores de la Cadena de Suministro.* Este artículo se puede consultar en la página 110, con el título **"El desarrollo de competencias del líder de seguridad en la cadena de suministro".**


110

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

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

Figura 1. Extracto del artículo publicado en la Guía de Seguridad para los actores de la cadena de suministro (DIJIN FSE, 2016).

Este mismo año, en el mes de diciembre, el Consejo de Seguridad en Cadena de Suministro (del cual soy titular) llevó a cabo el seminario internacional (México - Estados Unidos) denominado **"Dirección de proyectos, mitigación de riesgos, diseño de contramedidas y continuidad de operaciones en la cadena**

de suministro”, en el auditorio Senator Zaffirini Success Center, Laredo, en las instalaciones de la Texas International University, Laredo, Texas, Estados Unidos.

Figura 2. Presentación de la V edición de la Guía de Seguridad para los actores de la Cadena de Suministro, con la presencia y participación de oficiales adscritos al US Customs and Border Protection (US CBP) (Laredo, Texas, Estados Unidos, 2016).

Figura 3. Mayor Gelga Buitrago Martínez, entonces titular del Área de Asistencia y Cooperación para la Investigación Judicial y Frente de Seguridad Empresarial (DIJIN FSE), quien presenta la edición 2016 de la Guía de Seguridad para los actores de la Cadena de Suministro, con la presencia y participación de oficiales adscritos al US Customs and Border Protection (US CBP) (Laredo, Texas, Estados Unidos, 2016).

2017

Figura 4. Ing. Benjamín Grajeda Regalado, titular de la División de Gendarmería (derecha), quien recibe la Guía de Seguridad para los actores de la Cadena de Suministro, de manos del titular del Consejo de Seguridad en Cadena de Suministro, Eduardo Hernández Ruiz (México, abril 2017).

2018

Diplomado en Protección a Ciclos Productivos

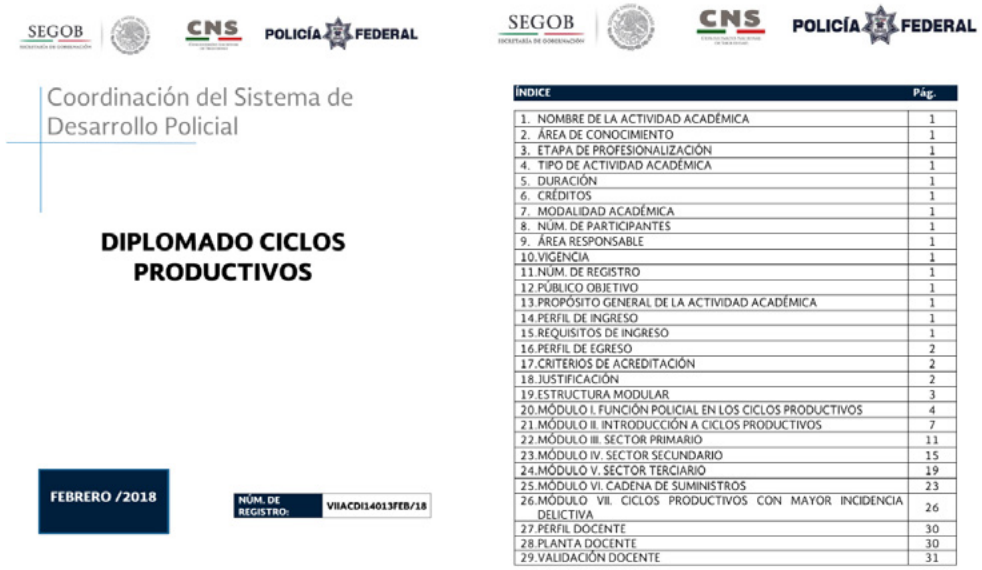
Los objetivos del diplomado en protección a ciclos productivos son:

a. Desarrollar competencias en el personal en activo de todas las divisiones de la Policía Federal en la interpretación de la norma ISO 28000.
b. Homologar criterios entre la autoridad y la industria, especialmente en programas de certificación de seguridad en cadena logística, como es el caso del programa Customs Trade Partnership Against Terrorism (CTPAT US CBP) y la certificación Operador Económico Autorizado del Servicio de Administración Tributaria (SAT Aduanas).
c. Fortalecer a las organizaciones de cualquier sector sus procesos logísticos críticos, de conformidad con la norma internacional ISO 28000, replicando este modelo en todas las organizaciones, especialmente en aquellos proveedores considerados críticos, como es el caso de empresas de transporte de carga terrestre, agencias aduanales, operadores logísticos, empresas de seguridad privada, entre otros.

El diplomado en protección a ciclos productivos tiene una duración total de 140 horas y está reservado a oficiales en activo de rango medio y superior, integrado por los siguientes módulos:

- Módulo 1. La función policial en los ciclos productivos
- Módulo 2. Introducción a ciclos productivos
- Módulo 3. Sector primario
- Módulo 4. Sector secundario
- Módulo 5. Sector terciario

- Módulo 6. ISO 28000, seguridad en la cadena de suministro
- Módulo 7. Ciclos productivos con mayor incidencia delictiva


Coordinación del Sistema de Desarrollo Policial

DIPLOMADO CICLOS PRODUCTIVOS

FEBRERO /2018

NÚM. DE REGISTRO: VIIACDI140113FEB/18

ÍNDICE	Pág.
1. NOMBRE DE LA ACTIVIDAD ACADÉMICA	1
2. ÁREA DE CONOCIMIENTO	1
3. ETAPA DE PROFESIONALIZACIÓN	1
4. TIPO DE ACTIVIDAD ACADÉMICA	1
5. DURACIÓN	1
6. CRÉDITOS	1
7. MODALIDAD ACADÉMICA	1
8. NÚM. DE PARTICIPANTES	1
9. ÁREA RESPONSABLE	1
10.VIGENCIA	1
11.NÚM. DE REGISTRO	1
12.PÚBLICO OBJETIVO	1
13.PROPÓSITO GENERAL DE LA ACTIVIDAD ACADÉMICA	1
14.PERFIL DE INGRESO	1
15.REQUISITOS DE INGRESO	1
16.PERFIL DE EGRESO	2
17.CRITERIOS DE ACREDITACIÓN	2
18.JUSTIFICACIÓN	2
19.ESTRUCTURA MODULAR	3
20.MÓDULO I. FUNCIÓN POLICIAL EN LOS CICLOS PRODUCTIVOS	4
21.MÓDULO II. INTRODUCCIÓN A CICLOS PRODUCTIVOS	7
22.MÓDULO III. SECTOR PRIMARIO	11
23.MÓDULO IV. SECTOR SECUNDARIO	15
24.MÓDULO V. SECTOR TERCIARIO	19
25.MÓDULO VI. CADENA DE SUMINISTROS	23
26.MÓDULO VII. CICLOS PRODUCTIVOS CON MAYOR INCIDENCIA DELICTIVA	26
27.PERFIL DOCENTE	30
28.PLANTA DOCENTE	30
29.VALIDACIÓN DOCENTE	31

Figura 5. Portada e índice del Diplomado en Protección a Ciclos Productivos. Policía Federal, División de Gendarmería. Acreditación con registro VIIACDI140113FEB/18 por el Sistema de Desarrollo Policial (SIDEPOL). Febrero del 2018.

El Diplomado en Protección a Ciclos Productivos fue desarrollado de conformidad con los siguientes instrumentos:

a. Norma internacional ISO 28000:2007, Sistema de Gestión de Seguridad en Cadena de Suministro
b. Programa Frente de Seguridad Empresarial de la Policía Nacional de Colombia (DIJIN FSE)
c. Guía de Seguridad en Cadena de Suministro 2016 (Policía Nacional de Colombia (DIJIN FSE)
d. Guía INTERPOL de colaboración Aduanas y Policía Federal (INTERPOL 2018)
e. Marco SAFE versión 2018 de la Organización Mundial de Aduanas (WCO SAFE 2018)
f. Guía de validación OEA (AEO WCO 2018)
g. Programa Partnership in Customs Academic Research and Development de la Organización Mundial de Aduanas (WCO PICARD 2019)

Figura 6. Guía de colaboración INTERPOL-Aduana Policía Federal (INTERPOL 2018).

2019

Actualmente en el 2019, existen ya siete generaciones con 300 oficiales egresados adscritos a las siete divisiones de la Policía Federal (Antidrogas, Inteligencia, Investigación, Fuerzas Federales, Seguridad Regional, Científica y, por supuesto, Gendarmería Nacional), formados como auditores de seguridad en la cadena de suministro.

Figura 7. Las siete divisiones de la Policía Federal de México durante la administración federal del 2012 al 2018.

Figura 8. Formación a personal de la Policía Federal en el módulo de ISO 28000.

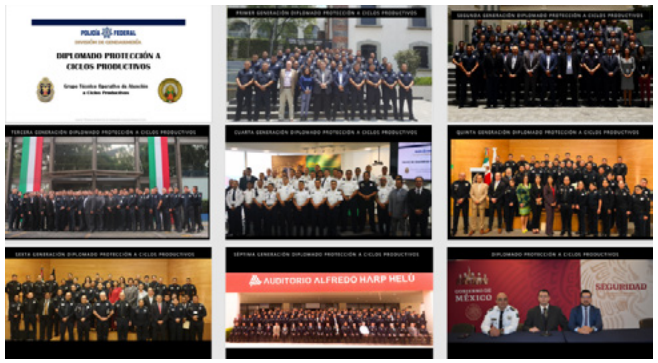


Figura 9. Las siete generaciones con 300 egresados del Diplomado Protección a Ciclos Productivos.

Figura 10. José Luis Vilchis Maya, Director de Protección a Ciclos Productivos, Gendarmería Nacional (izquierda); Eduardo Hernández Ruiz, Presidente del Consejo de Seguridad en Cadena de Suministro (centro), y José Ángel Vidaña Meraz,Director del Consejo de Seguridad en Cadena de Suministro (México, 2019).

Recomendamos a todos los países de cualquier región que desarrollen o repliquen el modelo denominado FRENTE DE SEGURIDAD EMPRESARIAL, con más de 19 años (POLICÍA NACIONAL DE COLOMBIA DIJIN), cuyo objetivo es crear un ESQUEMA DE RESPONSABILIDAD COMPARTIDA, que consiste en que la coordinación del sector privado y la autoridad trabajen por un mismo objetivo en materia de seguridad en cadena logística y de suministro, implementando la norma internacional ISO 28000:2007 (la cual será actualizada en el último trimestre del año 2020).

8.2. La certificación como Operador Económico Autorizado: Una herramienta para el crecimiento industrial

Por: Raúl Hernán Muriel Botero - Consultor en Seguridad

Para las autoridades aduaneras, el término "contaminación" hace referencia a la introducción de sustancias ilícitas o drogas en cargas que tienen un fin lícito. Este hecho puede afectar de manera importante la dinámica productiva de las empresas, máxime cuando los afectados son las personas que de una manera u otra están implicados en el proceso de transporte y producción. Esta afectación puede darse desde empleados del rango de un operario, hasta el nivel gerencial. Las cargas provenientes de países de riesgo, como el nuestro, son sometidas a procesos de auditoría más elevados, en correspondencia con los de otros países, lo cual disminuye la competitividad nacional y en particular la de las empresas. El Estado colombiano no ha sido ajeno a esta situación, y decidió adoptar desde el año 2011, de la Organización Mundial de Aduanas, el programa OPERADOR ECONÓMICO AUTORIZADO, como una forma de cooperación entre la figura empresa-Estado, para afianzar y facilitar el comercio global de manera segura.

Para el nivel directivo de la industria nacional, la producción de drogas y su oferta a nivel interno no debe de ser una situación de menor importancia; esto cobra mayor valor cuando dentro del funcionamiento de la empresa está la comercialización hacia el exterior. Colombia es el mayor productor de cocaína del mundo, pues supera a Perú y Bolivia, según la Organización de las Naciones Unidas y la Junta Internacional de Fiscalización de Estupefacientes. Este es un negocio lucrativo, que difícilmente puede ser igualado por otro de carácter legal; las ganancias del tráfico de estupefacientes pueden multiplicar por diez la inversión inicial.

Las autoridades aduaneras no tienen reparo por una empresa u otra a la hora de auditar el contenido de la carga; por lo tanto, se sobreentiende que no hay reparo a la hora de poner en evidencia una situación de riesgo, como la contaminación de la mercancía. No siendo el negocio de la droga una realidad desconocida para el Estado, este lucha día a día para aumentar los controles y disminuir el paso hacia otros países por medio de aeropuertos y puertos de embarque; es decir, Colombia optimiza a diario sus procesos de fiscalización y control, poniendo bajo la lupa a todos aquellos que tienen que ver con el transporte de mercancías a nivel internacional. Si bien para el Estado es menester apoyar el crecimiento económico del país, estas autoridades estatales están en función de la identificación de las irregularidades en los procesos mercantiles, tanto de empresas como de personas naturales; específicamente se especializan en la identificación de cualquier irregularidad que tenga que ver con el tráfico de sustancias psicoactivas, como se evidencia en la figura 1.

Figura 1. Fuente: EOM - El Orden Mundial

Estas continuas auditorías y la especialización del Estado para la identificación del tráfico de estupefacientes han hecho que los grupos al margen de la ley también se especialicen en la forma y el cómo transportan esas mercancías. El proceso de ensayo y error lleva más de siete décadas desarrollándose; comenzó como un tráfico espontáneo, sin restricciones en la segunda mitad del siglo XX, hasta un proceso minucioso y bien planificado en nuestra era; el tráfico tiene la misma finalidad: un cliente en países industrializados, que multiplica la inversión inicial en forma exponencial. Esta realidad no solo afecta moralmente el planteamiento del Estado, sino también el aparato productivo del país de manera transversal; aumenta la inseguridad, disminuye la competitividad, infiltra todos los niveles sociales y deforma la estructura del Estado social de derecho.

Para los industriales lo anterior cobra relevancia, pues no pueden crecer al margen de la realidad del sitio geográfico donde se encuentran. Las empresas que manejan cierta cantidad de recursos y transportan mercancías hacia otros países, están en la mira de los grupos que trafican estupefacientes a nivel internacional, son el canal perfecto para concretar sus negocios. Esta situación no se puede abordar desde un punto de vista simplista, como el depósito de un paquete con droga dentro de la carga; los delincuentes realizan estas actividades con minucia de relojero, para concretar la contaminación de una carga o aprovechar cargos críticos para lavar activos; estos toman en cuenta las vulnerabilidades de las empresas específicamente, actividades que están a la merced del azar o la informalidad. El ajuste y control de los procesos de selección, el seguimiento de cargos críticos, la verificación de proveedores y la auditoría de recursos económicos dificultan la materialización del riesgo.

Para sistematizar este proceso, múltiples entes del Estado otorgan a las empresas relacionadas con el comercio exterior la certificación como "OPERADOR ECONÓMICO AUTORIZADO"; por medio de esta se audita todo lo referente a la seguridad, con múltiples alcances, como recursos humanos, procesos, infraestructura, acceso, transporte, proveedores y asociados. Esta certificación tiene tal relevancia para el Gobierno Nacional, que ha decidido otorgar múltiples beneficios a las empresas que deciden voluntariamente certificarse, los cuales están pensados para aumentar la competitividad sin descuidar la lucha antidrogas, responsabilidad sinecuánime del Estado.

Las empresas certificadas como OPERADOR ECONÓMICO AUTORIZADO tienen beneficios tributarios, se les reduce el monto de garantías globales, actuación directa como declarantes exportadores ante la DIAN, implementación de canales especiales para la realización de operaciones de comercio exterior, disminución de inspecciones físicas por parte de la DIAN y la Policía Nacional, facilitación de la autorización del embarque en el lugar correspondiente, supresión de inspecciones intrusivas e implementación de procedimientos simplificados, entre otros. *Tomado de:* https://www.dian.gov.co/aduanas/oea/inicio/Documents/OEA_General.pdf

Lección aprendida - Eventos de contaminación de la carga

En este sentido y con el firme propósito de coadyuvar en la gestión del riesgo, Cosinte Ltda., en su portafolio de servicios, hace 23 años, viene implementando la gestión de riesgos y la fomentación de una seguridad preventiva en todos los niveles de la empresa.

Con este sentido, desde hace más de tres años, se incluyó en el portafolio de servicios de Cosinte el acompañamiento a las empresas para la certificación que otorga la DIAN como Operador Económico Autorizado, tiempo en el cual hemos logrado detectar la facilidad que tienen las bandas criminales para infiltrarse dentro de una organización y contaminar la carga de la misma, cuando no se tienen establecidas unas políticas de seguridad y gestión de riesgo adecuadas, que permitan detectar inconsistencias a tiempo.

La figura del OPERADOR ECONÓMICO AUTORIZADO (OEA) se le otorga a las empresas que están inmersas en el movimiento de mercancía a nivel internacional, y que mediante un adecuado control de riesgos en su cadena de suministro, obtiene el reconocimiento como un operador confiable y seguro, después de que se le realiza un proceso de validación por los entes competentes; en el caso de Colombia, la Dirección de Impuestos y Aduanas Nacionales (DIAN), la Policía Nacional y en algunos casos el Instituto Colombiano Agropecuario (ICA) y el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (INVIMA).

En este contexto, la certificación como OEA trae múltiples beneficios a las empresas, y en el momento en que los empresarios toman la decisión de certificarse, deben realizar gestiones a nivel interno en materia de gestión de riesgos, evaluando cada uno de los departamentos que componen la empresa

y determinando el nivel de seguridad en los mismos; entre otros aspectos para evaluar, se tienen: los controles de acceso físico, la seguridad del personal, la seguridad del contenedor y las unidades de carga, la seguridad en los procesos, la seguridad física, la seguridad en tecnología de la información, los asociados del negocio y demás ítems que permiten que se tenga una adecuada y oportuna gestión del riesgo.

En el marco de este contexto y en el desarrollo de nuestras actividades, hemos podido identificar que muchas empresas han fallado en materia de seguridad, lo que facilita a los criminales la infiltración y penetración de los escasos niveles de seguridad, lo cual tiene como consecuencia la materialización de la contaminación de carga en diversos escenarios, derivando esto en grandes repercusiones empresariales.

Por ejemplo, se han presentado casos en donde prestigiosas empresas que realizan diversas actividades industriales, han contado o bien con un deficiente nivel de seguridad o con fallas en los procesos de producción, distribución, comercialización y transporte de sus productos; en este sentido, hemos evidenciado que estas fallas logran poner en entredicho el "goodwill" de las empresas al desatender o descuidar los parámetros normativos internacionales de seguridad en la cadena de suministro.

En la práctica, las empresas se quedan relegadas a sus procedimientos comerciales tradicionales, y no implementan técnicas de gestión de riesgo que permitan adaptar su modelo de negocio, para evitar las emergentes formas de criminalidad en todos los niveles de la operación.

En Colombia, una empresa acostumbra a desarrollar sus procesos de producción y distribución con importante informalidad; esta situación fue aprovechada por agentes externos conocedores de esta deficiencia, quienes se infiltraron hasta utilizar los procesos de la empresa para el transporte de sustancias ilícitas. Los delincuentes utilizaron la razón social de ella y su reputación para alivianar los filtros de las autoridades competentes, sin tener en cuenta el sistemático proceso de inspección que se hace a nivel portuario. Esta situación afecta transversalmente el aspecto jurídico de la empresa, sin tener reparo en la jerarquía organizacional.

Ante la materialización de este riesgo, se pudo analizar lo siguiente:

¿Cómo pudo suceder?

La ausencia de procedimientos y protocolos de seguridad que garanticen una correcta trazabilidad de la operación conducen a la materialización del evento, de modo que se impacta económica y reputacionalmente a la organización.

Lo sucedido puso en evidencia una serie de errores que transversalmente facilitaron el evento; por ejemplo: la ausencia de acuerdos de seguridad entre el cliente y los proveedores, la falta de estudios de confiabilidad para la selección

de personal, la inexistencia de un sistema de gestión de riesgos que sea totalmente operativo y medible, aunado a los vacíos procedimentales y la falta de regulación de actividades críticas.

Lo anterior fue el resultado de la desintegración de las políticas, protocolos y procedimientos institucionales. Estos procesos deben estar anclados a un sistema de gestión de riesgos funcional, liderado por personal competente e idóneo en el manejo de riesgos.

Causas:

- Grupos al margen de la ley.
- Intereses desleales por parte de funcionarios de la empresa y del proveedor.
- Ausencia de acuerdos de seguridad entre la empresa y el proveedor de transporte.
- Falta de control de los estándares de seguridad exigidos por la empresa a los proveedores inmersos en la cadena de suministro.
- Inexistencia de estudios de confiabilidad al personal, tanto para el proceso de selección como para el seguimiento periódico de personal inmerso en actividades críticas (proveedores).

¿Dónde puede suceder?

Para las autoridades competentes, los escenarios que están sometidos a auditorías continuas; propiamente dicho, la certificación como Operador Económico Autorizado tiene menor riesgo de contaminación.

Las acciones implementadas por parte de la organización, después de este evento, fueron:

1. Adoptar la seguridad de los procesos institucionales como una política constante en todos los niveles de la operación.
2. Implementar un sistema de gestión de riesgos que sea transversal al negocio, los procesos y las personas, estableciendo directrices, políticas, procedimientos y protocolos funcionales que permitan administrar los distintos riesgos identificados.
3. Establecer una gerencia empresarial del riesgo, proceso realizado entre la alta dirección y el área administrativa y operativa, aplicando estrategias diseñadas para identificar eventos potenciales que puedan afectar la empresa, administrando los riesgos con el fin de proporcionar una seguridad e integridad razonables referentes al logro de los objetivos.
4. Acompañar a las empresas en sus planes hacia el futuro, reconociendo los errores del pasado y estableciendo procedimientos seguros en sus próximas operaciones.
5. Direccionar estratégicamente y fortalecer los planes de continuidad del negocio, con la finalidad de estructurar empresas resilientes y dinámicas, que potencialicen su infraestructura y procesos bajo un enfoque preventivo en la gestión del riesgo.

CARACTERÍSTICAS DE UNA EMPRESA VULNERABLE Y RESILIENTE	
EMPRESA VULNERABLE	**EMPRESA RESILIENTE**
El evento sorprende a la empresa.	La empresa cuenta con mecanismos de alerta temprana para tomar las medidas adecuadas ante la ocurrencia de un peligro.
La empresa no conoce los peligros que pueden amenazarla.	La empresa ha identificado sus peligros, elaborando un mapa de riesgo y plan para tratamientos de los riesgos (PTR).
La empresa no sabe qué hacer en caso de un evento grave.	La empresa ha identificado sus peligros y está preparada para actuar de forma eficaz y eficiente.
La empresa no está preparada para la ocurrencia de un evento grave.	La empresa ha conformado un equipo especializado en caso de un evento grave.
La empresa adopta una actitud pasiva ante la ocurrencia de un evento grave, considerándolo como fortuito.	Encabezada por el dinamismo de sus directivos, la empresa toma conciencia de la posibilidad de prepararse para afrontar a un evento grave y reducir su impacto.
La empresa está en un entorno hostil y peligroso.	La empresa se reubica o genera estrategias proactivas paraser más segura o implementa medidas estructurales para minimizar los riesgos.

Cuadro 1. Análisis de riesgo-Aspectos empresariales.

La seguridad a nivel preventivo es el pilar de Cosinte Ltda. En nuestra trayectoria, la prestación del servicio a reconocidas empresas en los ámbitos nacional e internacional ha permitido la creación de una conciencia organizacional y la generación de políticas de gestión de riesgo que previenen la materialización de este.

8.3. Cadenas de suministro seguras

Por: Julián Andrés Puentes B., CPP, PSP[1]

Ha sido tradición que las organizaciones enfoquen sus esfuerzos en la venta de bienes y servicios, lo cual ha llevado a que gran parte de las tareas se oriente hacia la producción o la construcción de experiencias para el cliente. Pese a esto, el concepto de seguridad en la cadena de suministro se ha centrado, en particular, en procesos de recibo y de despacho, y en años recientes en los procesos de exportación e importación como referentes del comercio internacional.

Profesionales de la seguridad han hallado en la cadena de suministro un nicho interesante, debido a algunas iniciativas, como la Asociación de Aduanas y Comercio contra el Terrorismo (CTPAT[2], por sus sigla en inglés) y el Operador Económico Autorizado (OEA[3]), que contemplan algunas medidas de seguridad, las cuales en su mayoría son casos de seguridad física.

Estos tienen la ventaja de que permiten ver cómo los modelos de recibo, despacho y transporte tienen muchas similitudes en todas las operaciones, lo cual ha hecho que la labor de consultoría replique modelos, por encontrar "estadios comunes" de la operación, pero lo anterior plantea la duda: ¿la cadena de suministro solo se limita a este tipo de operación?

La definición de cadena de suministro

De acuerdo con la definición que ofrece la norma ISO 28000:2008, la cadena de suministro consiste en la relación bilateral entre las organizaciones, las personas, los procesos, la logística, la tecnología y los recursos que están involucrados en actividades que crean valor a partir de la adquisición de materiales en la entrega de productos y servicios.

Según lo anterior, cada organización, sin importar cuál es su objeto social y si entrega un bien o un servicio, necesariamente debe tener una cadena de suministro. Es posible que la organización la llame por otro nombre o que no considere que va más allá de la operación logística.

Así, las organizaciones deben establecer su cadena de suministro en todos los niveles de sus procesos de producción o de servicio, y determinar con qué

[1] Magíster en Seguridad y Defensa Nacionales, especialista en Administración de la Seguridad, certificado CPP, PSP por ASIS Internacional, experto en Sistemas de Gestión en Operaciones de Seguridad, Seguridad en la Cadena de Suministro y Gobernanza.

[2] Programa voluntario del gobierno de los Estados Unidos, con el propósito de construir relaciones de cooperación comercial mejorando la seguridad en la frontera.

[3] Iniciativa de control aduanero internacional, liderada por la Organización Mundial de Aduanas para facilitar el comercio seguro entre países.

controles reducirán la incertidumbre sobre la continuidad de sus operaciones, teniendo claros cuáles son los puntos críticos de control, la planeación de la demanda, el ciclo de la orden, el proceso de planeación de ventas y operaciones (S&OP), la logística de reversa, las relaciones con los clientes y proveedores, la disminución del desperdicio mediante metodologías como *Lean Six Sigma*[4], Agile SCRUM[5] y la aplicación de habilidades obtenidas según el Certificado en Gestión de la Cadena de Suministro (CSCM, por su sigla en inglés) y la certificación como Profesional en Gestión de Proyectos (PMP, por su sigla en inglés).

Las organizaciones con cierto nivel de madurez presumen que para que sus operaciones mantengan la continuidad, la seguridad de la cadena de suministro es vital. Cuando hacen esto, piensan tanto en la protección del contenedor o el monitoreo satelital del vehículo que se desplaza hacia el puerto, como en muchos otros asuntos: asegurar que se suministre el personal, la capacitación, el entrenamiento, la construcción de conocimiento, la herramienta, la maquinaria, la materia prima, los insumos. También, que se mantenga activa la producción, cuidando el almacenamiento, la infraestructura, los métodos y las técnicas propias, el modelo Investigación + Desarrollo + Innovación (I+D+I), y que se consolide un mercado frente a los nuevos competidores, la amenaza de productos sustitutos, la guerra comercial, la dinámica del cambio de divisas y de los aranceles, el poder de negociación con proveedores y compradores, y por último la confianza de la red de distribución y la entrega física o digital.

Con todos los aspectos mencionados antes, la seguridad de la cadena de suministro es la seguridad de la misma organización, al pretender gestionar los riesgos que podrían afectar de forma negativa la continuidad de las operaciones.

Para lograr una aproximación eficaz a ese contexto hay que conocer la estrategia organizacional, la cual establece el patrón clave para la dirección. Este define y apoya los objetivos a largo plazo.

La dirección, a su vez, estipula el porqué de la existencia del negocio, y cómo este se mantendrá estable y viable[6].

La organización, entonces, define presupuestos de capital y de gasto para que se mantengan los riesgos controlados o en un estado en que se puedan manejar. Luego se determina que la función de seguridad o de control de riesgos de seguridad ayuda a que se cumplan los objetivos organizacionales, al reportar directamente a la alta gerencia.

4 Estrategia que integra la detección y eliminación de fallos o defectos, y el aumento de la velocidad de los procesos eliminando ineficiencias y optimizando la creación del valor.

5 Proceso que aplica un conjunto de buenas prácticas, para trabajar colaborativamente y obtener el mejor resultado de un proyecto.

6 Definición del Manual de Protección de Activos (POA, por su sigla en inglés), ASIS International.

Esta función, por tanto, debe ser rentable bajo el enfoque costo-beneficio. Tiene que haber estrategias de retorno del gasto –y no de la inversión[7]–, indicadores de gestión, análisis de datos. Con lo anterior, la seguridad en las cadenas de suministro se describe como la puesta en marcha de la práctica de estándares y principios que, cuando se aplican de forma constante, mantienen en su lugar los riesgos corporativos.

Los riesgos en la cadena de suministro

- Estos pueden ser los siguientes:
- Piratería terrestre
- Suplantación
- Contaminación de la carga
- Contratación de empleados deshonestos
- Vinculación de clientes y proveedores que afectan reputacionalmente la relación comercial, la falsificación y el contrabando

Hay otros riesgos que se deben estudiar con más cuidado, interpretando el contexto, los factores y su probabilidad, además de los costos que están asociados a la pérdida, y qué tan viable es implementar contramedidas, que consideren elementos y cálculos objetivos que incluyan razones de rentabilidad, yendo más allá de una simple percepción de un analista o consultor.

La seguridad en las cadenas de suministro requiere de un gran esfuerzo y la concentración de profesionales con sabiduría, con destrezas técnicas y conocimientos avanzados de seguridad física, seguridad del personal, seguridad de la información, seguridad de las operaciones, seguridad reputacional, manejo de crisis e investigaciones.

También, destrezas gerenciales en la administración del recurso escaso, mediante la gestión de presupuesto, e indicadores de rentabilidad y habilidades para negociar con personas, en la conducción de equipos de trabajo, la generación de conciencia de seguridad y la influencia en el liderazgo ejecutivo de la organización, que contribuyan al diagnóstico, el diseño, la implementación y la evaluación de programas de prevención, control y recuperación de pérdidas en cada uno de los eslabones.

[7] Las compras de seguridad, contablemente se registra el gasto; la inversión genera una expectativa de utilidad o renta medida en dinero.

8.4. La cadena de suministro y su papel clave en la norma ISO 18788:2015

Por: Julián Andrés Puentes B., CPP, PSP[1]

Pese a contar con un buen número de normas que regulan la prestación de servicios de seguridad privada, en Colombia existía la necesidad de ampliar la cobertura recurriendo a las herramientas de autorregulación, tal como lo han hecho empresas prestadoras de servicios en otros países, las cuales se han acogido a normas como el Código Internacional de Conducta de Empresas Prestadoras de Servicios de Seguridad[2] (ICoC, por su sigla en inglés) o como Compañías de Seguridad Privada[3] (PSC.1, por su sigla en inglés), de ASIS International.

Es así como, en respuesta a la necesidad de proteger los derechos humanos en las operaciones de seguridad, surge la norma ISO 18788:2015. Es ese su espíritu, en especial en aquellos territorios en donde existe una gobernabilidad débil y hay un socavamiento del Estado de derecho.

El fin de la norma, entonces, es el de cuidar la reputación de las empresas que son contratadas para ofrecer este servicio, teniendo en cuenta que cuando se posee un arma de fuego se transfiere una autoridad y hay una expectativa con el control que esto pueda generar, lo cual ubica al operador en una situación de riesgo potencial de violar los derechos humanos en la ejecución de su actividad.

Aquellas empresas que se encuentran en el proceso de implementación de la norma han identificado que, para alcanzar este propósito, tienen que conseguir que toda la organización se comprometa con esa tarea. ¿Cómo? Logrando que todos los procesos interactúen entre sí, entendiendo que para que la organización preste un servicio tiene que haber un proceso, el cual va desde participar en una adjudicación del contrato, hasta que se le pague por el servicio prestado.

Todo lo que ocurre entre ese principio y ese final se entiende como la cadena de suministro[4]; es decir, una serie de actividades que se desarrollan de manera

[1] Magíster en Seguridad y Defensa Nacionales, especialista en Administración de la Seguridad, certificado CPP, PSP por ASIS Internacional, experto en Sistemas de Gestión en Operaciones de Seguridad, Seguridad en la Cadena de Suministro y Gobernanza.

[2] Código que establece principios y normas internacionales para la provisión responsable de servicios de seguridad privada en entornos complejos.

[3] Estándar de gestión para la calidad de las operaciones de empresas de seguridad privada incorporando requisitos de protección de derechos humanos

[4] Relación en doble vía entre organizaciones, personas, procesos, logística, tecnología y recursos involucrados en actividades que crean valor a partir de la adquisición de materiales a través de la entrega de productos y servicios.

sistemática, en las que se involucran todos los procesos misionales, de dirección y de apoyo para la entrega final del producto, y su respectivo pago.

Las empresas tienen que tener claro el mapa de su cadena de suministro, identificando las entradas y las salidas, los recursos que tienen disponibles para la prestación del servicio, los subcontratistas, las actividades, las modalidades y los medios para que ello ocurra.

Lo anterior reportará beneficios, tales como la identificación de las brechas que hay en el proceso del servicio, así como las actividades aisladas que operan bajo sus propios códigos, ignorando los de la alta dirección; es así como las organizaciones de este sector que se postulen a la certificación de la norma ISO 18788:2015, deberán considerar el mapa de su cadena de suministro como un insumo fundamental del sistema de gestión de operaciones, para identificar riesgos y oportunidades en la protección de los derechos humanos y la reputación de las partes interesadas.

Las bondades de la cadena de suministro

En el contexto interno de las organizaciones, la cadena de suministro es clave porque ayuda a identificar todas las partes que tienen algo que ver con la prestación del servicio. También, para tener clara cuál es la participación de las áreas de apoyo, misión y dirección en su diseño y ejecución, ayudando a que las que trabajan de manera aislada y sin indicadores se vinculen en la aplicación de las medidas en los puntos críticos de control[5], para cumplir con las expectativas de las partes interesadas, para proteger los derechos humanos y para que se conserve el buen nombre y la reputación de la empresa y de su cliente a la vez.

Otra ventaja de este proceso es que permite hacer foco en las brechas o desconexiones en etapas importantes, pues con su ejecución descubre actividades consideradas por la alta dirección como útiles para conseguir los objetivos estratégicos, pero que en la práctica no son ejecutadas o se hacen de acuerdo con el criterio, el buen juicio o el sentido común –que en ocasiones es el menos común de los sentidos– de quienes lideran cada proceso. Al interactuar cada eslabón es cuando surgen errores en la comunicación, y algunas de las tareas previas quedan mal hechas, lo cual impacta de forma negativa en el producto o servicio que se desea.

La cadena de suministro también es fundamental en la identificación, el análisis y la evaluación de riesgos[6], pues evidencia los posibles problemas que se pueden presentar en cada eslabón, los cuales, por un lado, dificultan la consecución de los objetivos de la organización, y del otro, la exponen a riesgos reputacionales que se derivan de la violación de los derechos humanos, los cuales afectan las libertades de cada individuo.

5 Punto, paso o proceso en el cual se pueden aplicar controles y prevenir una amenaza o peligro, eliminarlo o reducirlo a niveles aceptables.

6 Tres elementos que componen el proceso global de la valoración de riesgos.

La norma tiene como requisito la política y la declaración de aplicabilidad; esto determina la expectativa de la organización y la manera en la que pretende satisfacerla, tanto en la calidad del servicio como en la protección de los derechos humanos y de la reputación de la empresa.

Por último, la cadena de suministro ayuda a descubrir las actividades, las modalidades y los medios que se utilizan en la prestación del servicio, que le aporta a la organización para conseguir el alcance que pretende de acuerdo con su objeto social; en ese proceso se encuentran las intenciones de la corporación frente al producto o servicio que entregará, y se define el alcance de la certificación del sistema de operaciones en seguridad privada:

Prestación de servicios de vigilancia y seguridad privada en las modalidades fija, móvil, escolta y transporte de valores; servicios con armas y sin ellas; medio humano y tecnológico; medio canino y servicios conexos de asesoría, consultoría e investigaciones.

Entender a una organización que presta servicios de seguridad privada, desde la esencia de su negocio, invita a construir o a hacer un mapa –tal como lo sugiere la norma– de cada una de las actividades lógicas, en secuencia o paralelamente con la interacción de las partes, para saber cómo las entradas (es decir, las expectativas de las partes interesadas) se transforman en salidas (producto o servicio conforme).

El mapa de las actividades sirve para identificar eficazmente la cadena de suministro. En tal virtud, la alta dirección o el liderazgo ejecutivo entenderán de manera integral qué ocurre aguas arriba de los procesos que son considerados como “esencia del negocio”, y hacia abajo, una vez que se sale del control operacional directo.

ISBN 978-958-98894-7-3

2019