DIOS Y PATRIA

Es un honor ser Policía

HERRAMIENTA DE SEGURIDAD PARA LOS ACTORES DE LA CADENA DE SUMINISTRO

PAUTAS PARA LA PREVENCIÓN CRIMINAL

VII EDICIÓN

2022

DIOS Y PATRIA
Es un honor ser Policía

HERRAMIENTA DE SEGURIDAD PARA LOS ACTORES DE LA CADENA DE SUMINISTRO

PAUTAS PARA LA PREVENCIÓN CRIMINAL

VII EDICIÓN

2022

Ministerio de Defensa Nacional
Policía Nacional de Colombia

ISBN 978-628-95321-0-4

Mayor general
Henry Armando Sanabria Cely
Director General Policía Nacional de Colombia

Brigadier general
Yackeline Navarro Ordoñez
Subdirectora Policía Nacional de Colombia

Coronel
Olga Patricia Salazar Sánchez
Directora de Investigación Criminal e INTERPOL

Coronel
German Iván Romero Sanabria
Subdirector de Investigación Criminal

Teniente Coronel
Héctor Ruíz Arias
Jefe de Investigación Judicial

Mayor
Sonia Reyes Sánchez
Jefe Frente de Seguridad Empresarial

Corrección de Estilo
PIENSA BTL S.A.S.

Diseño e impresión
PIENSA BTL S.A.S.
Bogotá, D. C., Colombia, noviembre de 2022

AGRADECIMIENTOS

Esta publicación no hubiera sido posible sin el interés, dedicación y aporte intelectual de las personas y entidades que realizaron su valioso aporte en la elaboración de la VII Edición de la Herramienta de Seguridad para los Actores de la Cadena de Suministro, que desde hace más de dos décadas han contribuido con la implementación de buenas prácticas del sector productivo de bienes y servicios, la prevención criminal mediante el fortalecimiento de la gestión del riesgo así como la prevención en seguridad, impactando positivamente los diferentes actores presentes en la operación de las empresas.

A los integrantes del Comité Editorial, que aportaron, redactaron y consolidaron el contenido de este documento; al Equipo de Trabajo del Frente de Seguridad Empresarial; al Maestro Carlos Ariza Mora, Consultor Internacional en Seguridad Privada; al Ingeniero Jhon Jairo Mónoga, Auditor para el Sistema de Gestión Antisoborno; al señor Jairo Andrés Rodríguez Guerrero, Director General Grupo OET; al señor Mayor (RA) Carlos Alfonso Boshell Norman, Auditor Internacional de Certificación BASC; a los Señores Eduardo Hernández Ruiz, José Ángel Vidaña Meraz (†), Jorge Jaramillo Baena y las Señoras Rosa María Jiménez Mendoza y Mercedes Escudero Carmona (Consejo de Seguridad en Cadena de Suministro); Zuly Gloria Pacheco Ruiz (Presidente de la Comisión de enlace con la Guardia Nacional de México de CANACINTRA); Al Señor Mariano Sánchez CEO – Socio fundador Risk Internacional; Brigadier General de la Reserva Activa Juan Carlos Buitrago Arias - Founder & CEO Strategos BIP; al Instituto Nacional de Investigación y Prevención de Fraude – INIF; Al Ingeniero John Jairo Gutiérrez- Auditor de Sistemas de Gestión de ICONTEC.

PRÓLOGO

Conocimiento e interacción son fundamentales para la Prevención

Prevención, disuasión y acción contra el delito, bajo el marco del respeto por la Constitución Nacional, las leyes, los reglamentos, los derechos humanos y el ejercicio de las libertades, así como la exigencia frente al cumplimiento de los deberes, son los lineamientos que guían a la Policía Nacional en su misión.
Para el desarrollo de las acciones institucionales, las cuales procuran la convivencia y seguridad en Colombia, son fundamentales las prácticas investigativas, formativas, consultivas y de construcción conjunta que se desarrollan con la comunidad internacional y nacional.

La interacción entre ciudadanía e Institución fortalece la superación de los objetivos trazados y consolida la presencia policial en cada uno de los territorios del país; brindando confianza y legitimidad de cara a la superación de variables que, en el corto, mediano o largo plazo se transforman en multiplicadoras de conductas contrarias a la ley.

En este entorno de construcción conjunta, generación, transmisión e interacción con el conocimiento, permanece la esencia de la prevención, la cual vincula la misionalidad con el contexto; trascendiendo hacia la puesta en marcha de acciones que permiten la gestión eficiente de los riesgos asociados a la seguridad.

Consciente de la importancia que representan para Colombia el sector productivo y la cadena de suministro, la Policía Nacional publica, cada tres años, este documento que incluye la visión internacional, la experiencia institucional y la prospectiva como contribución al desarrollo de la productividad, en beneficio de los colombianos.

Herramienta que plasma las relaciones armónicas y de trabajo coordinado con los diferentes sectores económicos del país, la articulación con expertos en seguridad y los amplios esfuerzos que, desde la institucionalidad, se realizan para brindar conocimiento moderno e innovador, en procura de fortalecer la seguridad en la cadena de suministro.
La lectura, comprensión y práctica del contenido investigativo presente en la "VII Edición de la Herramienta de Seguridad para los Actores de la Cadena de Suministro", contribuirá a la consolidación de Colombia como una fuerza productiva a nivel mundial.

DIOS Y PATRIA

¡ES UN HONOR SER POLICÍA!

Mayor general
Henry Armando Sanabria Cely
Director General Policía Nacional de Colombia

INTRODUCCIÓN

Las nuevas dinámicas utilizadas por los actores criminales que afectan la convivencia y seguridad ciudadana requieren de una modernización tecnológica y física de factores estratégicos y operaciones de la Policía Nacional, en especial, aquellos enfocados en reducir los índices de criminalidad del sector comercial, industrial y económico del país.

La articulación del sector público y privado en Colombia en materia de seguridad ha permitido la identificación de estas "nuevas dinámicas", individualización y judicialización de quien la implementa y modificación de estrategias de prevención del delito en el sector económico ofreciendo una respuesta oportuna y contundente.

La seguridad informática es tan relevante para todos los sectores sociales y económicos, que garantizar la seguridad de la información se hace retador para los organismos de seguridad internacional; nuestra Policía Nacional en aras de fortalecer las políticas de seguridad cibernética, cuenta con un Equipo de Respuesta a Incidentes de Seguridad Informática, el cual tiene el objetivo apoyar las estratégicas de ciberseguridad y ciberdefensa en Colombia, como soporte fundamental en la prevención e investigación de la seguridad informática empresarial.

Este es el momento y hora de aportar conjuntamente en la VII Edición de la Herramienta de Seguridad para los Actores en la Cadena de Suministro, fortaleciendo la participación de la sociedad, contribuyendo en la Seguridad Humana, construyendo principios y valores ciudadanos, previniendo la afectación a sus actividades comerciales y mitigando las circunstancias que conllevan a la comisión de conductas penales.

La Policía Nacional saluda con complacencia a los miles de empresarios que han participado de la mano con el Frente de Seguridad Empresarial; exaltamos

su esfuerzo inalienable en la construcción de un mejor país y su aporte a la convivencia y seguridad de todas y todos los colombianos.

Cuenten siempre con una Policía Nacional innovadora, integra, disciplinada y capacitada en la protección de derechos y garantías contempladas en nuestro Estado Social de Derecho, así como profesionalizada en gerencia, diseño e implementación de políticas de seguridad ciudadana contribuyendo en su seguridad empresarial.

Coronel
Olga Patricia Salazar Sánchez
Directora de Investigación Criminal e INTERPOL

OBJETIVOS

General

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

Especificos

1. 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.

2. Contextualizar al lector a cerca del Programa de Transparencia y Ética Empresarial como una herramienta obligatoria para la prevención y lucha contra la corrupción en los sectores público y privado Colombia - ley 2195 de 2022.

3. Socializar las Responsabilidades Post- Certificación “Operador Económico Autorizado”.

4. Ayudar al empresario a aprender cómo gestionar el conflicto de intereses desde los valores éticos.

5. Dar a conocer el aporte de los Seguros a la Seguridad en la Cadena de Suministro.

6. Establecer la importacia de transversalidad y correlación de las normas ISO en la continuidad de operaciones en cadena de suministro.

7. Publicar buenas prácticas en ciberseguridad a los empresarios en Colombia, que permitan controlar los eventos que impactan negativamente el desarrollo de sus actividades.

8. Brindar herramientas para Demostrar Confiabilidad NTC ISO/IEC 27701:2020 Técnicas de seguridad. Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad de la información. Requisitos y directrices.

9. Enseñar los criterios para gestionar la continuidad del negocio en operaciones de Cadena de Suministro.

10. Explicar como la buena debida diligencia es una herramienta para la prevención de riesgos y en algunos casos para conceptos que impliquen la validación de una empresa o persona previa a la firma de un contrato.

11. Brindar al empresario una serie de actividades que promuevan la adopción de los sistemas SIPLAFT y SARLAFT dentro de la compañía.

12. 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.

ABREVIATURAS

BASC	Business Alliance for Secure Commerce
BCMS	Business Continuity Management System
DITRA	Dirección de Tránsito y Transporte
DIRAN	Direccion de Antinarcótico
DIJIN	Dirección de Investigación Criminal e Interpol
FESEM	Frente de Seguridad Empresarial DIJIN
ISO	International Organization for Standardization
ICA	Instituto Colombiano Agropecuario
POLFA	Policía Fiscal y Aduanera
SOAT	Seguro Obligatorio de Accidentes de Tránsito
SIPLAFT	Sistema Integral para la Prevención del Lavado de Activos y de la Financiación del Terrorismo
SARLAFT	Sistema de Administración del Riesgo del Lavado de Activos y Financiación del Terrorismo
SAGRILAFT	Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos y Financiación Del Terrorismo
SCBMS	Supply Chain Business Continuity Management System
OFAC	Oficina para el Control de Activos Extranjeros
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OEA	Operador Económico Autorizado
ONUDI	Organización de las Naciones Unidas para el Desarrollo Industrial
UNODC	Oficina de las Naciones Unidas contra la Droga y el Delito
UIAF	Unidad de Información y Análisis Financiero
RUAF	Registro Único de Afiliados
FOSYGA	Fondo de Solidaridad y Garantía
FBI	Federal Bureau of Investigation
FODA	Fortalezas, Oportunidades, Debilidades, Amenazas
FASECOLDA	Federación de Aseguradores Colombianos
INTERPOL	Internacional Criminal Police Organization
IEC	International Electrotechnical Commission
DEA	Drug Enforcement Administration
DIAN	Dirección de Impuestos y Aduanas Nacionales
MTPD	Periodo Máximo Tolerable de Interrupción
MTD	Maximun Tolerable Downtime

ROS	Reporte de Operaciones Sospechosas
ROA	Return On Assets
RUES	Registro Único Empresarial y Social
DHS	United States Department of Homeland Security
DANE	Departamento Administrativo Nacional de Estadística
RUNT	Registro Único Nacional de Transito
ROS	Reportes de Operaciones Sospechosas
RTO	Recovery Time Objective
RPO	Recovery Point Objective
BCP	Banco de Crédito del Perú
HLS	High Level Structure
CCTV	Circuito Cerrado de Televisión
CCIT	Cámara Colombiana de Informática y Telecomunicaciones
CCB	Cámara de Comercio de Bogotá
CPTED	Crime Prevention Through Environmental Design
CANACINTRA	Cámara Nacional de la Industria de Transformación
ANDI	Asociación Nacional de Empresarios de Colombia
ADEN	Acrónimo de Asociación de Discapacitados de Enfermedades Neurológicas
ASIS	Análisis de Situación de Salud
ALSUM	Asociación Latinoamericana de Seguros Marítimos
AMERIPOL	Comunidad de Policías de América
PEP	Permiso Especial de Permanencia
GAFI	Grupo de Acción Financiera Internacional
ESCIB	Estrategia Integral de Ciberseguridad
EUROPOL	Agencia de la Unión Europea en Materia policial
EQ	Ethics Quotient
WRT	Work Recovery Time

CAPÍTULO 1

FRENTE DE SEGURIDAD EMPRESARIAL

Por: Mayor Sonia Reyes Sánchez, Intendente Jefe Jhon Rodas Londoño, Intendente Pedro Mujica Gavilán, Intendente Willy Salcedo Tole, Subintendente Javier Pérez Roa, Subintendente Ferney Rojas Lemus, Patrullero Lina Aguilar Santacruz, Patrullero Mónica Bermeo Vásquez, Patrullero José Castro Molina.

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 y que estén 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.

- Jornadas de sensibilización: espacios inclusivos creados 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.

- Operador exclusivo: atención personalizada de un 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, contribuyendo al cumplimiento de los objetivos estratégicos institucionales.

Requisitos de vinculación

ETAPA I
Inscripción

- Formulario de inscripción y declaraciones del solicitante_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 pre vinculación

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

Criterios de visita técnica pre vinculación: 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, 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 de archivo 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.

Despliegue a nivel nacional

El Frente de Seguridad Empresarial, cuenta con una cobertura integral del servicio a nivel nacional, focalizando Gestores de Seguridad Empresarial en cada una de las Seccionales de Investigación Criminal, permitiendo así, un acompañamiento dedicado en cada una de las jurisdicciones locales, departamentales y regionales, garantizando de esta manera un acompañamiento permanente que permita mejorar los canales de comunicación y la correcta articulación del proceso y el sector empresarial.

CAPÍTULO 2

PROGRAMA DE TRANSPARENCIA Y ÉTICA EMPRESARIAL, HERRAMIENTA OBLIGATORIA PARA LA PREVENCIÓN Y LUCHA CONTRA LA CORRUPCIÓN EN LOS SECTORES PÚBLICO Y PRIVADO

COLOMBIA - LEY 2195 de 2022

Miguel Velásquez Olea
Director Ejecutivo BASC Bogotá - Colombia
Gestor Editorial.

Por: Carlos Alfonso Boshell Norman
Auditor Internacional de Certificación BASC

Uno de los mayores anhelos de las personas de bien, es que la transparencia a nivel global aumente, aunque esto parece ser una simple utopía. Transparencia Internacional ha publicado su **Índice de Percepción de la Corrupción 2021,** que mide los niveles de penetración de la corrupción en el sector público en 180 países de todo el mundo, entre los resultados, dos tercios de los países han obtenido una puntuación inferior a 50, con una media mundial de 43, que se mantiene sin cambios por décimo año consecutivo, es decir que en 131 países no han hecho ningún progreso significativo contra la corrupción en la última década, lo que en realidad nos muestra es que pareciera no existir un decido compromiso real para lograr cambios significativos, se hace fundamental poner en marcha iniciativas que fortalezcan la transparencia, la integridad y la rendición de cuentas en las instituciones públicas y en el sector privado, de lo contrario los progresos se esfumarán rápidamente.

Esta lucha comienza a organizarse y unificarse a partir de la convención de Mérida (México) en 2003 de las Naciones Unidas contra la corrupción, que preocupada por la gravedad de los problemas y las amenazas que plantea la corrupción para la estabilidad y seguridad de las sociedades al socavar las instituciones y los valores de la democracia, la ética y la justicia y al comprometer el desarrollo sostenible y el imperio de la ley, por los vínculos entre la corrupción y otras formas de delincuencia, en particular la delincuencia organizada y la delincuencia económica, incluido el blanqueo de dinero. Los casos de corrupción que entrañan vastas cantidades de activos, los cuales pueden constituir una proporción importante de los recursos de los Estados, y que amenazan la estabilidad política y el desarrollo sostenible de estos. Se decide que, a fin de aumentar la sensibilización respecto de la corrupción, así como del papel que puede desempeñar la Convención para combatirla y prevenirla, se proclame el 9 de diciembre Día Internacional contra la Corrupción.

Convencidos que corrupción dejo de ser un problema local para convertirse en un fenómeno transnacional que afecta sociedades y economías, esencial en la cooperación internacional para prevenirla y luchar contra ella, se requiere un enfoque amplio y multidisciplinario para prevenir y combatir eficazmente la corrupción. La disponibilidad de asistencia técnica puede desempeñar un papel importante para que los Estados estén en mejores condiciones de poder prevenir y combatir eficazmente la corrupción, entre otras cosas fortaleciendo sus capacidades y creando instituciones. El enriquecimiento personal ilícito puede ser particularmente nocivo para las instituciones democráticas, las economías nacionales y el imperio de la ley.

Tomando nota con reconocimiento de los instrumentos multilaterales encaminados a prevenir y combatir la corrupción, incluidos, entre otros la Convención Interamericana contra la Corrupción, aprobada por la Organización de los Estados Americanos el 29 de marzo de 1996, el convenio relativo a la lucha contra los actos de corrupción en los que estén implicados funcionarios de las Comunidades Europeas o de los Estados Miembros de la Unión Europea, aprobado por el Consejo de la Unión Europea el 26 de mayo de 1997, el Convenio sobre la lucha contra el soborno de los funcionarios públicos extranjeros en las transacciones comerciales internacionales, aprobado por la Organización de Cooperación y Desarrollo Económicos el 21 de noviembre de 1997, el convenio de derecho penal sobre la corrupción, aprobado por el Comité de Ministros del Consejo de Europa el 27 de enero de 1999, el Convenio de derecho civil sobre la corrupción, aprobado por el Comité de Ministros del Consejo de Europa el 4 de noviembre de 1999 y la Convención de la Unión Africana para prevenir y combatir la corrupción, aprobada por los Jefes de Estado y de Gobierno de la Unión Africana el 12 de julio de 2003.

La Convención Anticohecho de la OCDE y el Grupo de Trabajo sobre Cohecho para combatir el cohecho de servidores públicos extranjeros en transacciones comerciales internacionales de la OCDE, es un acuerdo legalmente vinculante; los países que se unen a la Convención y acuerdan establecer como delito el cohecho de un servidor público extranjero en su legislación nacional e implementar políticas efectivas para evitar, detectar, investigar y sancionar el cohecho internacional.

La Convención Anticohecho de la OCDE es el primer y único instrumento internacional anticorrupción que se enfoca en el lado “oferente” de la corrupción, es decir la persona o entidad que ofrece, promete u otorga una dádiva. Este preciso enfoque ha permitido a la OCDE convertirse en la autoridad más destacada del mundo contra el cohecho en transacciones comerciales internacionales.

Ahora bien, las ciencias sociales definen la corrupción bajo un efecto paraguas, simplemente para demostrar la gran complejidad que esto representa, sin embargo el concepto más antiguo indica “decadencia” en términos filosóficos, platónicos, donde el poder corrompe al hombre y es el hombre el que termina utilizando el poder para un beneficio personal y egoísta versus un beneficio común, empíricamente es muy difícil definir que es corrupción porque es un fenómeno multifactorial, pensemos por un momento que puede ser una red

de actos individuales o colectivos, comportamientos legales o ilegales, que actual simultáneamente y a lo largo del tiempo de una forma organizada y sistemática para llevar a cabo un acto o diversos actos de corrupción. Entre la basta literatura académica y política se destacan tres enfoques para definir la corrupción que podemos abordarla analizarlo en la forma normativa, también a partir de sus características y magnitud y como fenómeno social.

Desde el punto de vista **normativo** se contemplan conductas de tipo ilegales categorizadas, por ejemplo: tráfico de influencias, cohecho, peculado, desvío de recursos públicos, enriquecimiento ilícito, soborno, por nombrar algunas, que son las formas como los servidores públicos pueden extraer recursos para su propio beneficio, o también usar el poder para favorecer a sus amigos o familiares. Pero los actos de corrupción se componen de actos legales e ilegales y por eso la ciencias sociales han creado categorías para definir la **magnitud de la corrupción:** la gran corrupción, corrupción estructural, corrupción sistémica o endémica, pequeña corrupción, rentismo y clientelismo. En cuanto al **fenómeno social,** por ejemplo el hurto de recursos públicos de manera organizada dentro de las instituciones de gobierno y la distribución de programas sociales a cambio de votos o apoyo electoral.

La definición de corrupción más operativa y utilizada es la del Banco Mundial y la de Transparencia Internacional que habla de la corrupción como la **utilización del poder para un beneficio personal** y esta definición tiene una connotación adicional filosófica muy antigua pero que funciona actualmente para comprender básicamente qué se entiende cuando se habla de corrupción. Sin embargo, los esfuerzos por definir y comprender qué es la corrupción, deben ir mucho más allá de una idea filosófica o de un concepto teórico, necesitamos construir modelos cualitativos, cuantitativos y estadísticos que nos permitan entender la corrupción desde sus orígenes, desde sus causas, desde la forma, para poder modelarla, prevenirla, predecirla, y ese es un gran reto.

Ley 2195 de 2022, herramienta en la lucha contra la corrupción.

Por primera vez en nuestro país se brinda una herramienta que permite sancionar a las personas jurídicas, levantar el velo corporativo de las personas jurídicas que se prestan para actos de corrupción, aplicar sanciones para que nunca más vuelvan a contratar con el estado, también para que se atribuyan

responsabilidades a sus gestores y directivos que se prestan para ese contubernio como es la corrupción.

Enfocada a fortalecer la capacidad para sancionar de la justicia en nuestro país, esta ley permite dar otro paso que es trascendental al permitir aplicar extinción de dominio y enajenación temprana de bienes mal habidos producto de actos de corrupción. También define la obligación de conocer quiénes son los beneficiarios finales de los actos de corrupción, además de brindar lineamientos a los aspectos de la pedagogía buscando mejores herramientas de prevención, la protección de la niñez en la correcta utilización de los recursos públicos para la alimentación de los niños del sistema educativo de nuestro país. También podemos visualizar otro principio y es el de un estado abierto donde a partir del escrutinio de sus contratistas y del conocimiento de las bases de datos relacionales, donde se pueda encontrar la cantidad de contratos y la idoneidad de los mismos para su ejecución, se pueda recuperar la confianza ciudadana y el respeto por lo público.

El objeto de esta ley está en adoptar disposiciones tendientes a prevenir los actos de corrupción, a reforzar la articulación, a la coordinación de las entidades del estado, a recuperar los daños ocasionados por dichos actos con el fin de asegurar y promover la cultura de la legalidad e integridad y a recuperar la confianza ciudadana y el respeto por lo público.

Impactos en los sectores público y privado de esta ley.

Al revisar el impacto de la ley 2195 de 2022 para las organizaciones públicas y personas jurídicas del sector privado en materia de transparencia, prevención y lucha contra la corrupción debemos enfocarnos en tres ejes: **prevención, sanción y fortalecimiento institucional**.

Entre los principales aspectos a destacar establece que todas las superintendencias deberán, bajo ciertos criterios, obligar a sus vigilados a adoptar

programas de transparencia y ética empresarial, ampliando así la facultad de regulación y sanción que hoy solamente ostentan la superintendencia de sociedades y la superintendencia de salud en cuanto a estos programas, esperando que en un plazo de seis meses siguiente a la expedición de esta ley, las superintendencias deberán determinar el deber a cargo de sus vigilados e identificar a los beneficiarios finales de sus contrapartes. Lo anterior amplia el universo de empresas obligadas a implementar procedimientos de debida diligencia, en cuanto a sanciones administrativas en materia de soborno transnacional, además de la multa hasta por 200.000 SMMLV a quienes incurran en esta conducta, incorporando igualmente el criterio **del mayor valor entre el beneficio obtenido y el pretendido**.

Programas de transparencia y ética empresarial.

La promulgación de la ley 2195 de 2022 trajo nuevas regulaciones, donde una de las principales fue la ampliación en la **obligación de implementar un Programa de Transparencia y Ética Empresarial (PTEE)** a las organizaciones públicas, y en el sector privado a los vigilados por cualquier superintendencia o regulador, en el caso de las Pymes y MiPymes a las que se les deberán establecer programas de acompañamiento que faciliten la elaboración e implementación de los programas de transparencia y ética empresarial, que en coordinación con la Secretaría de Transparencia de la Presidencia de la República brindarán los lineamientos mínimos de dicho programa.

También se prevé la posibilidad de articular el Sistema de Administración de Riesgos con el Programa de Transparencia y Ética Empresarial, que serán evaluados y actualizados al menos cada 4 años, igualmente, es importante resaltar la inclusión del parágrafo a "los estándares internacionales y

nuevas prácticas", dentro de los cuales debemos considerar los estándares internacionales de la Norma BASC, Sistema de Gestión en Control y Seguridad, ISO37001:2016 Sistema Gestión Antisoborno, ISO37301:2021 Sistema Gestión de Cumplimiento, entre otros, además de la inclusión de los auditores internos, jefes de control interno, que deberán verificar el cumplimiento y eficacia del programa, incluyendo la obligación del Revisor Fiscal quien deberá valorar el programa y emitir su opinión sobre el mismo.

Con este contexto se hace importante y necesario que todos los interesados (sector público y privado), conozcan los aspectos básicos normativos, técnicos, metodológicos y de capacitación que contienen estos planes de transparencia y ética empresarial.

Modelos de programas de transparencia y ética empresarial empleados en Colombia.

Comencemos por definir que es un Programa de Ética Empresarial, y para esto nos vamos a referir al concepto emitido en la "guía destinada a poner en marcha programas de ética empresarial para la prevención de las conductas previstas en el artículo 20 de la ley 1778 de 2016" emitida por la Superintendencia de Sociedades en su circular 100-00003 del 2016 y nos indica que "Son los procedimientos específicos a cargo del Oficial de Cumplimiento, encaminados a poner en funcionamiento las Políticas de Cumplimiento, con el fin de identificar, detectar, prevenir, gestionar y mitigar los riesgos de Soborno Transnacional, así como otros que se relacionen con cualquier acto de corrupción que pueda afectar a una Persona Jurídica", que para ajustarla al objeto de la ley 2195 de 2022 estaría encaminada a identificar, detectar, prevenir, gestionar y mitigar los riesgos de Corrupción.

No olvidemos que esta ley nos abre la posibilidad que en aquellas personas jurídicas que tengan implementado un sistema integral de administración de riesgos, pueden **articularlo** (NO REEMPLAZAR) al **programa de transparencia y ética empresarial** de forma tal que incluya los riesgos que mediante el mismo se pretenden mitigar.

Las superintendencias o autoridades de inspección, vigilancia o control de la rama ejecutiva en coordinación con la Secretaría de Transparencia de la Presidencia de la República, determinarán los lineamientos mínimos que

deben prever los programas de transparencia y ética empresarial con el fin de estandarizar las acciones, las políticas, los métodos, procedimientos, mecanismos de prevención, control, evaluación y de mejoramiento continuo. Dichos lineamientos serán evaluados y actualizados, de **conformidad con los estándares internacionales y nuevas prácticas** que fortalezcan los programas de transparencia y ética empresarial, al menos cada cuatro (4) años.

Será necesario monitorear el desarrollo de la Ley y con eso conocer qué cambios normativos y regulatorios se pueden llegar a implementar, por ahora la invitación está enfocada que a partir de los gremios como por ejemplo BASC, el Frente de Seguridad Empresarial de la DIJIN y otros, impulsen las buenas practicas, diseño, implementación y desarrollo y acompañamiento de los programas de transparencia y ética empresarial enfocados a la prevención de las actividades de corrupción y soborno.

Revisemos las buenas prácticas que podremos utilizar en estos programas:

1. Plan Anticorrupción y de Atención al Ciudadano-PAAC

Se creó con el artículo 73 del Estatuto Anticorrupción y se concibe como una herramienta para la prevención de la corrupción en el que cada entidad a nivel nacional, departamental y municipal, plasma anualmente su apuesta institucional de lucha contra la corrupción. La metodología para su elaboración está contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano", realizada por la Secretaria de Transparencia, en articulación con el Departamento Administrativo de la Función Pública (DAFP) y el Departamento Nacional de Planeación DNP. El Plan Anticorrupción y Atención a la Ciudadanía (PAAC) lo componen: mapa de riesgos de corrupción, estrategia antitrámites, rendición de cuentas, mecanismos para mejorar la atención al ciudadano, transparencia y acceso a la información y las iniciativas adicionales que estimen conveniente incluir las entidades. Cuenta con Mapa de Riesgos de Corrupción – MRC, que se concibe como el conjunto de actividades que le permiten a una entidad identificar, analizar evaluar y mitigar la ocurrencia de riesgos de corrupción en los procesos de su gestión. La metodología para la elaboración del MRC está contenida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas elaborada por el Departamento Administrativo de la Función Pública (DAFP), Ministerio de Tecnologías de la Información y las Comunicaciones

(MinTic) y la Secretaria de Transparencia. En cuanto a los mecanismos jurídicos útiles para combatir la corrupción, el acceso a la información es un derecho de rango constitucional, a través del cual toda persona puede solicitar y recibir información de las autoridades públicas, conforme a lo consignado en los artículos 74 y 209 de la Constitución Política y en la Ley 1712 de 2014. El mencionado derecho, está indisolublemente ligado al principio de publicidad que rige la administración pública y se ajusta a los parámetros constitucionales que permean al derecho de petición, de información y el libre acceso a los documentos públicos.

2. Pactos de Transparencia - Sector Público

Desde la Vicepresidencia de la República y la Secretaría de Transparencia se han firmado Pactos de Transparencia e Integridad con diferentes alcaldías y gobernaciones del país. En este contexto, las diferentes gobernaciones y alcaldías municipales, se comprometen a avanzar en compromisos que son claves para fomentar la transparencia y luchar efectivamente contra la corrupción en el país, entre los cuales se destacan los siguientes aspectos:

2.1 Hacer uso del SECOP II, la tienda virtual del Estado y cumplir a cabalidad los principios de la contratación estatal.

2.2 Avanzar en el proceso de implementación de la Ley de Transparencia y Acceso a la Información Pública, definiendo responsables, indicadores y metas concretas.

2.3 Publicar en su página web las declaraciones de bienes, rentas y los conflictos de intereses de los funcionarios obligados en la Ley 2013 de 2019.

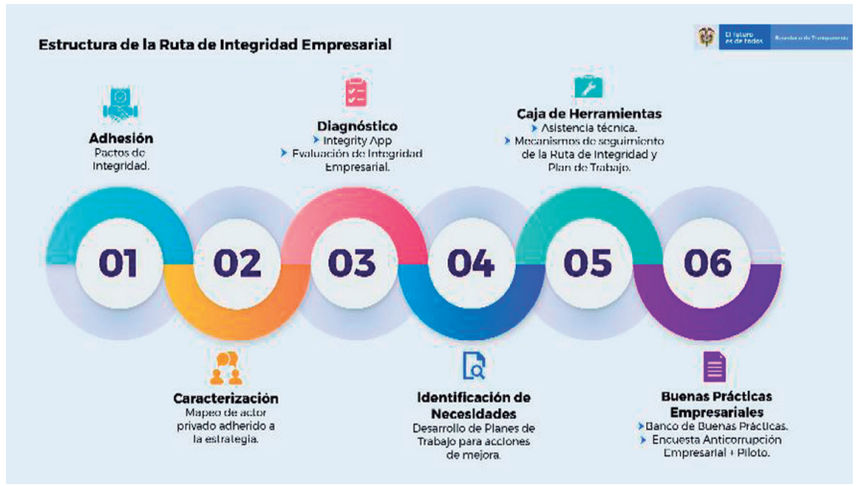
2.4 Crear un canal antifraude y de denuncia segura para el ciudadano, protegiendo al denunciante. Este canal debe estar articulado con la Red Interinstitucional de Transparencia y Anticorrupción – RITA.

2.5 Implementar acciones para el tratamiento sistemático de la corrupción que permitan atacar el fenómeno desde el manejo de riesgos, la articulación con entidades territoriales y órganos de control territorial, el fortalecimiento de la cultura de la integridad, la analítica de datos y la caracterización de las modalidades de corrupción que se hubiesen presentado en el territorio, entre otros aspectos que contienen los pactos.

Para acompañar y asesorar a las gobernaciones y alcaldías del país en el cumplimiento del mencionado Pacto, la Secretaría de Transparencia de la Presidencia de la República, ha brindado asistencia técnica integral para entidades territoriales, que se complementan con procesos de capacitaciones para garantizar el cumplimiento de lo acordado y para fortalecer las capacidades institucionales con el fin de fomentar la transparencia y luchar efectivamente contra la corrupción en los territorios. En el mismo sentido, se ha brindado una serie de recomendaciones para incluir aspectos claves en materia de transparencia y lucha contra la corrupción en los planes de desarrollo departamentales, distritales y municipales y para la correcta implementación de la Red Interinstitucional de Transparencia y Anticorrupción – RITA.

3. Ruta de Integridad Empresarial

La Ruta de Integridad Empresarial es una estrategia de la Secretaria de Transparencia que permite a los actores privados diseñar, implementar, socializar y divulgar mecanismos y políticas de transparencia empresarial que permitan contribuir a la construcción de integridad en el sector, agregando



valor a su cadena, mayor confianza con grupos de interés y mejores prácticas empresariales en la lucha contra la corrupción.

Esta estrategia busca promover en el sector empresarial la cultura de la integridad, como una medida que permita proporcionar un marco para las buenas prácticas empresariales y estrategias de gestión de riesgos que contrarresten cualquier práctica de corrupción.

Esta Ruta brindará herramientas necesarias con asistencia técnica a los actores privados para incorporar, fortalecer y mantener mecanismos de transparencia e integridad empresarial con el fin de mitigar conflictos y problemas en la gestión y así lograr un mejor clima organizacional, credibilidad y confianza con sus grupos de interés, una mejora en la reputación y estabilidad en el mercado, una justa y libre competencia y un valor agregado a la sociedad.

Son bienvenidos todos los actores privados que tengan dentro de su estrategia corporativa crear y gestionar compromisos en la lucha contra la corrupción y hacia la adopción, al interior de estos, de prácticas de transparencia, ética e integridad, como un factor estratégico para asegurar la sostenibilidad y competitividad de los negocios y contribuir así a la construcción de lo público. Mediante la manifestación de su interés y compromiso en gestionar y fortalecer capacidades institucionales, a través de la aplicación de insumos que ofrece la Caja de Herramientas de la Ruta de Integridad Empresarial, que ayudan a tener un panorama mucho más estructurado en la generación de resultados, es decir, cambios derivados directamente de las medidas implementadas con mejoras en los mecanismos y políticas de transparencia e integridad corporativa y su relacionamiento con todos los grupos de interés. Desde la Secretaría se gestionará el proceso para la firma de compromisos de integridad empresarial a través del Pacto de Integridad, y una vez firmado se desarrollarán los pasos establecidos en la Ruta de Integridad Empresarial.

4. Los Programas de Transparencia y Ética Empresarial (PTEE) Supersociedades

Conforme lo prevé el último inciso del artículo 23 de la Ley 1778, la Superintendencia de Sociedades, mediante Resolución No. 100-002657 del 25 julio de 2016, determinó las Sociedades Vigiladas que están obligadas a adoptar Programas de Ética Empresarial. Para este propósito, la Superintendencia tuvo en cuenta, criterios tales como el valor de los activos, ingresos, número de empleados y objeto social de la persona jurídica, entre otros, los obligados que deberían haber implementado un PTEE que está enfocado a la identificación

de riesgos de soborno transnacional, son las sociedades vigiladas que a 31 de diciembre del año anterior hayan realizado transacciones con personas naturales o jurídicas extranjeras, por valores desde 100 SMMLV; y hayan obtenido ingresos totales o activos totales desde 30.000 SMMLV.

Por su parte, deben implementar PTEE enfocados en la identificación de riesgos de corrupción, empresas que a 31 de diciembre del año anterior hayan celebrado contratos con entidades estatales por cuantías desde 500 SMMLV y hayan obtenido ingresos totales o activos totales desde 30.000 SMMLV, empresas de los sectores farmacéutico, infraestructura y construcción, manufacturero, minero-energético, TICs, comercio de vehículos, y accesorios, o de actividades auxiliares a servicios financieros que a 31 de diciembre del año anterior hayan celebrado contratos con entidades estatales, por una cuantía igual o superior a 500 SMMLV y hayan obtenido ingresos totales desde 3.000 SMMLV o activos totales desde 5.000 SMMLV.

Propuesta de buenas prácticas para implementar un PTEE corrupción

Pretendiendo adaptar el modelo guía de buenas prácticas a partir de un "Programa de Transparencia y Ética Empresarial" (PTEE), dirigido a mitigar los riesgos específicos relacionados con el Soborno Transnacional y que nos permita mitigar los riesgos de corrupción en nuestras organizaciones deberíamos tener en cuenta inicialmente el COMPROMISO DE LOS ALTOS DIRECTIVOS EN LA PREVENCIÓN DE LA CORRUPCIÓN SOBORNO TRANSNACIONAL quienes serán los encargados de promover una cultura de transparencia e integridad en la cual la corrupción, sea considerada inaceptable.

Para los efectos anteriores, los altos directivos o asociados que tengan funciones de dirección y administración en la Persona Jurídica, según sea el caso, deberían al menos poner en marcha las Políticas de Cumplimiento y el Programa de Ética Empresarial asumiendo un compromiso dirigido a la prevención de la Corrupción así como de cualquiera de sus prácticas, de forma tal que la Persona Jurídica pueda llevar a cabo sus negocios de manera ética, transparente y honesta, asegurar el suministro de los recursos económicos, humanos y tecnológicos que requiera el Oficial de Cumplimiento para el cumplimiento de su labor, ordenando las acciones pertinentes contra los administradores y los asociados que tengan funciones de dirección y administración en la Persona Jurídica, cuando cualquiera de los anteriores infrinja lo previsto en el Programa

de Ética Empresarial, además de liderar una estrategia de comunicación adecuada para garantizar la divulgación eficaz de las Políticas de Cumplimiento y del Programa de Ética Empresarial en los Empleados, Asociados, Contratistas y la ciudadanía en general.

La segunda tarea vital a tener en cuenta, la encontramos en la EVALUACIÓN DE LOS RIESGOS RELACIONADOS CON LA CORRUPCIÓN, esta debe ser la piedra angular de un Programa de Ética Empresarial efectivo. Mediante la Investigación de los riesgos de corrupción se deben establecer los factores que podrían repercutir en nuestra organización independiente del tamaño, actividades o mercados relevantes donde realice sus operaciones. Le permitirá establecer en qué orden y con qué prioridad deberán adoptarse medidas para mitigar adecuadamente tales riesgos, identificando y evaluando sus riesgos por medio de diagnósticos independientes, tales como procedimientos periódicos de Debida Diligencia y de auditoria de cumplimiento, que deberán adelantarse con recursos económicos y humanos que sean suficientes para cumplir el objetivo de una correcta evaluación.

La tercera tarea es el diseño e implementación del PROGRAMA DE ÉTICA EMPRESARIAL, donde demos tener en cuenta que el Programa de Ética Empresarial se sujete a las siguientes pautas:

4.1. Elaborarse con fundamento en la evaluación exhaustiva de los riesgos particulares de corrupción y de cualquier otra práctica corrupta a los que esté expuesta una Persona Jurídica.

4.2. Organizarse de forma tal, que sea posible identificar, detectar, prevenir y mitigar riesgos relacionados con la corrupción.

4.3. Regular los aspectos relacionados con la identificación y evaluación de riesgos relacionados con la corrupción y delinear los procedimientos generales para adelantar procesos de Debida Diligencia y Auditoría de Cumplimiento.

4.4. Constar por escrito, en un Manual de Cumplimiento, cuyo texto deberá ser objeto de actualización cada vez que se presenten cambios en la actividad de la Persona Jurídica que alteren o puedan alterar el grado de riesgo de corrupción.

4.5. Establecer sistemas de control y auditoria, conforme lo determina el

artículo 207 del Código de Comercio y de conformidad con los estándares internacionales y nuevas prácticas aplicables.

4.6. Asignarles a los Empleados que estén expuestos a los riesgos de corrupción deberes específicos, relacionados con la prevención de esta conducta.

4.7. Poner en marcha procedimientos sancionatorios adecuados y efectivos, de conformidad con las normas laborales y disciplinarias, respecto de infracciones al Programa de Ética Empresarial cometidas por cualquier empleado.

4.8. Establecer la creación de canales apropiados para permitir que cualquier persona informe, de manera confidencial y segura acerca de actividades sospechosas relacionadas con la corrupción en cualquiera de sus prácticas.

4.9. Facilitar que los asociados de negocio tengan acceso y conozcan las Políticas de Cumplimiento y el Programa de Ética Empresarial de la persona jurídica.

4.10. Acordar con los asociados de negocio que tengan un mayor grado de exposición al riesgo de corrupción, compromisos expresos para prevenirla.

La cuarta tarea a tener en cuenta es la designación de un **OFICIAL O ENCARGADO DE CUMPLIMIENTO,** siendo un individuo con la idoneidad, experiencia y liderazgo requeridos para gestionar tales riesgos y cualquier otro que se relacione con un acto de corrupción, independientemente de la forma de gobierno corporativo que hubiere sido adoptada por la Persona Jurídica, es recomendable delegar, preferiblemente, en uno de los empleados con funciones de dirección, confianza o manejo, que dependa únicamente de los altos directivos y tenga acceso directo a estos últimos. Además, es importante que tal funcionario cuente con la autonomía y los recursos humanos, tecnológicos y económicos requeridos para poner en marcha el respectivo Programa de Ética Empresarial.

La quinta actividad a desarrollar es la **DEBIDA DILIGENCIA** que está orientada a suministrarle a la persona jurídica los elementos necesarios para identificar y evaluar los riesgos de corrupción que estén relacionados con las actividades de

una persona jurídica, sus sociedades subordinadas o los asociados de negocios, cuando estos últimos estén expuestos a un alto grado a este riesgo. Por medio de la revisión periódica de aspectos legales, contables o financieros. La Debida Diligencia también podrá tener como finalidad la verificación del buen crédito o la reputación de sus asociados orientarse a la identificación y evaluación de riesgos de corrupción relacionados con la actividad que desarrolle la Persona Jurídica.

El sexto paso es desarrollar un **CONTROL Y SUPERVISIÓN DE LAS POLÍTICAS DE CUMPLIMIENTO Y PROGRAMA DE ÉTICA EMPRESARIAL,** para este efecto, la Alta Dirección deberá poner en marcha mecanismos que le permitan a los encargados de las auditorias o control interno incluir en su plan anual de auditoría la verificación del cumplimiento y eficacia de los programas de transparencia y ética empresarial. Evaluando mecanismos de prevención, control, evaluación y de mejoramiento continuo. Dichos lineamientos serán evaluados y actualizados, de conformidad con los estándares internacionales y nuevas prácticas que fortalezcan los programas de transparencia y ética empresarial, al menos cada cuatro (4) años y el revisor fiscal, cuando se tuviere, debe valorar los programas de transparencia y ética empresarial y emitir opinión sobre los mismos.

La séptima actividad está en la **DIVULGACIÓN DE LAS POLÍTICAS DE CUMPLIMIENTO Y PROGRAMA DE ÉTICA EMPRESARIAL,** para evitar de manera efectiva las actividades de corrupción los empleados, administradores, asociados de negocio que deberán conocer adecuadamente el Programa de Ética Empresarial. Para este efecto, la persona jurídica deberá poner en marcha mecanismos idóneos para la correcta comunicación de tal programa. Una apropiada estrategia de comunicación, debería incluir capacitaciones a los empleados de la persona jurídica y a los trabajadores de los contratistas.

Por ultimo debemos implementar **CANALES DE COMUNICACIÓN** como mecanismos que les permitan a los empleados, asociados, contratistas e individuos vinculados a los anteriores, así como a cualquier persona que tenga conocimiento de una conducta de corrupción o de prácticas relacionadas con la persona jurídica, la posibilidad de reportar de manera confidencial infracciones a la Ley Anti Corrupción y al Programa de Ética Empresarial. Estos mecanismos deberán incentivar a los denunciantes a reportar tales infracciones sin temor a posibles represalias de otros funcionarios de la persona jurídica. Por lo tanto, el Oficial de Cumplimiento deberá adoptar las medidas correspondientes para asegurar la confidencialidad de los reportes recibidos, Tomar medidas

para proteger a los empleados en relación con posibles represalias de las que puedan ser objeto como consecuencia de la decisión que éstos adopten en el sentido de no involucrarse en conductas de Soborno Transnacional.

En conclusión, un buen Programa de Ética Empresarial deberá permitirle a una Persona Jurídica, prevenir, detectar y corregir situaciones que tengan el potencial de convertirse en una infracción a la Ley Anti Corrupción. Así las cosas, para que un Programa de Ética Empresarial sea considerado efectivo, deberá cuando menos estar diseñado con fundamento en una evaluación exhaustiva de los riesgos de corrupción que cada Persona Jurídica tenga intención de mitigar, ponerse en marcha el compromiso decidido de los altos directivos para que sus empleados, asociados de negocio y administradores, realicen acciones que sean efectivas para prevenir cualquier otra práctica corrupta, estableciendo mecanismos dirigidos a la ejecución de actividades periódicas de auditoría de cumplimiento y debida diligencia para verificar la efectividad del Programa de Transparencia y Ética Empresarial y cuando resulte necesario, proceder a su modificación y actualización, de manera que se adecue a los cambios que acontezcan en su entorno particular.

CAPÍTULO 3

RESPONSABILIDADES POSTCERTIFICACIÓN “OPERADOR ECONÓMICO AUTORIZADO”

Por: Carlos Ariza, Lic. Ps., Magister en Criminología, Consultor internacional en Seguridad Privada.

El reto de preparar una organización para poder obtener cualquier certificación es una tarea que requiere el compromiso de todos los equipos involucrados directa o indirectamente, se genera un gasto desde lo físico, lo mental, lo financiero y en general en los recursos que están orientados a trabajar, diseñar, implementar y actualizar todos y cada uno de los requisitos que se necesitan para colgarse esa medalla que va a contribuir con el mejoramiento de las condiciones de seguridad y en los cumplimientos internos y ante los clientes.

Los equipos comprometidos, trabajan en pro de cumplir las condiciones de acuerdo con los requerimientos y esto va en paralelo con las responsabilidades que tienen en su día a día. Estas no se pueden descuidar, pero a pesar de ello, se mueven ya que la motivación de sacar adelante un proyecto como este en particular relacionado con el Operador Económico Autorizado "OEA", genera un gran aprendizaje personal que se quedará para lo largo de sus vidas profesionales y que puede ser de mucha utilidad en un nuevo cargo o posición que ocupe. OEA es un reto que lleva a los miembros de la organización a exigirse en cuanto a la creatividad, capacidad de tomar decisiones en lo grupal, en lo individual, que reta el conocimiento y la curiosidad, que pone a prueba la paciencia y el conocimiento de las personas que han sido vinculadas al proceso y que da la satisfacción del deber cumplido al obtenerla.

Lo importante es tener en cuenta que una vez se obtiene la resolución, ahí no termina la responsabilidad, por el contrario, inicia una responsabilidad mucho más grande ya que se deben orientar los esfuerzos a no perderla por falta de control o de gestión. No se puede bajar la guardia ya que, sí bien es cierto las contramedidas de seguridad que se implementaron fueron acordes a unas exigencias muy fuertes, estas deben continuar en la misma forma e incluso en ocasiones volverse más robustas según evolucione el nivel de riesgo.

La invitación con esta publicación es la de recordar la importancia de mantener algunos controles clave para así administrar y gestionar los riesgos asociados a la Seguridad en la Cadena de Suministro. Desde hace unos años Colombia a través del convenio con la Organización mundial de Aduanas, ha llevado a los diferentes actores de la Cadena de Suministro internacional hacia un nuevo y dinámico proceso en el que la Certificación como Operador Económico Autorizado, en la que se armonizan todos los procesos Logísticos y de Seguridad para fortalecer las operaciones de importación y exportación de las compañías, teniendo como beneficios la disminución de los costos, celeridad en los tiempos de entrega en la recepción o salida de los materiales o productos terminados

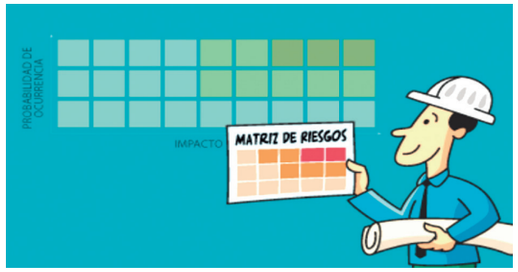
y también en los aspectos relacionados con la seguridad en la Cadena de suministro.

Muchas compañías en Colombia han logrado culminar con éxito ese tan exigente camino y han obtenido la tan anhelada certificación, sin embrago; es de recordar que este es solo el principio de una gran responsabilidad, ya que; como es bien sabido en un país con un alto riesgo de contaminación de la carga por diversos factores como narcóticos, insumos restringidos, dinero, armas, municiones, entre otros; los ojos deben estar puestos en cómo mantener las contramedidas de seguridad adecuadas y suficientes para poder continuar generando factores de disuasión en contra de los grupos al margen de la ley que están buscando permanentemente formas de traficar de una manera rápida y segura para ellos.

Por ello es importante tener en cuenta que, para poder seguir siendo miembros de tan selecto grupo de Operadores Económicos Autorizados, se deben seguir pautas, procesos, protocolos, políticas y procedimientos para reducir la probabilidad de ser seleccionados como blancos potenciales de los delincuentes.

En ese orden de ideas, desde la experiencia de haber sido parte de un gran equipo de personas que gestionó y logró la certificación, se pone sobre la mesa una serie de elementos de los esquemas de seguridad para que se reduzca la probabilidad de ocurrencia de incidentes en la seguridad de la cadena de suministro internacional y que de ocurrir,z se logre mitigar los impactos asociados a estos incidentes:

1. Actualización de las matrices de riesgo:



1.1 Es necesario realizar una reunión con el Comité Gestor de OEA dentro de la organización para revisar sí todos los riesgos existentes están vigentes y asociados a la realidad de la operación, a los riesgos de seguridad y a las medidas de seguridad tomadas. Los riesgos son

dinámicos y pueden cambiar de manera sutil o abrupta y es por ello que los responsables de OEA deben estar atentos a la evolución, cambio o incluso la aparición de un nuevo riesgo que no había sido contemplado en la matriz. Un claro ejemplo es lo que ocurrió con la pandemia, que pocas o casi ninguna compañía lo tenía mapeado y ha generado muchos cambios no sólo en temas de procedimientos sino también de procesos y estándares.

1.2 Siempre se sugiere que una matriz de riesgos sea revisada o evaluada cuando ocurren las siguientes variables:

1.2.1 Ocurrencia de un incidente en el que las contramedidas de seguridad no hayan sido suficientes o adecuadas

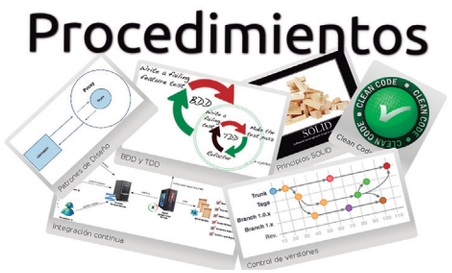
1.2.2 Que mediante la realización de un ejercicio de simulacro "pruebas de vulnerabilidad o penetración", se detecte que las contramedidas de seguridad no son suficientes o están ausentes

1.2.3 Cuando se presenten cambios en los factores de riesgo en la zona en la que se tiene operación

1.2.4 Al realizarse la apertura de una nueva operación, que implique evaluar los niveles de riesgo reales y las contramedidas de seguridad a implementar

1.2.5 En caso de recibirse amenazas directas o indirectas que comprometan la seguridad de las personas y de la operación

2. Revisión y actualización de los procedimientos de seguridad:



2.1 Fueron diseñados con base en las exigencias del programa implementado por la DIAN (Dirección de Impuestos Nacionales) y para obtener la certificación, fueron revisados y avalados, sin embargo; pasó un buen tiempo entre lo uno y lo otro y por ello que se invita a revisarlos de nuevo para evaluar

sí continúan o no alineados a los riesgos identificados en las matrices de riesgo.

2.2 Los procedimientos de seguridad hacen parte directa de la Seguridad en la Cadena de Suministro y por ende, el responsable de seguridad de cada organización certificada debe ser una pieza activa y se e debe mantener informado en tiempo y forma, de todos los cambios que vayan a ocurrir, es decir; que cuando se tomen decisiones de agregar, retirar, ajustar o cerrar procesos, el responsable de seguridad debe formar parte del equipo de expertos para que pueda desde el inicio identificar sí es necesario o no cambiar, ajustar o incluso eliminar procedimientos asociados a la seguridad de la cadena de suministro internacional.

2.3 Los procedimientos de seguridad buscan siempre que se reduzca la probabilidad de materialización de un riesgo, por lo que se debe asegurar que son socializados y que los empleados los tienen claros y presentes, al mantenerlos actualizados logramos el compromiso de los integrantes de la organización y con esto, se crea, ajusta y mantiene la Cultura de seguridad dentro y fuera de la organización.

2.4 La revisión y actualización debe involucrar a todas las partes interesadas, significa que tanto las áreas internas como las externas que hacen parte de la operación de logística deben ser involucradas, ya que es necesario que los procesos de los *stakeholders* que integran la operación de logística, pero que no están dentro de la organización, alineen sus procedimientos a la par con los de la organización a la cual le prestan sus servicios como operadores logísticos.

2.5 Otro asunto relevante, es que, por temas de rotación, separación de la compañía o decisión de los colaboradores, en estos últimos dos años, se ha generado una rotación dentro de las organizaciones y se pudo haber dejado de lado la actualización de los datos de contacto claves dentro de la organización para dar a conocer incidentes o novedades.

2.6 Por último, en este punto, se requiere que por lo menos una vez cada dos meses, el Comité que se creó para obtener la certificación se reúna, para revisar que los indicadores asociados a estos procedimientos se estén llevando a cabo y se compartan las novedades que se presentan para poder realizar los ajustes pertinentes, cerrando así las brechas oportunamente para evitar que se materialicen los riesgos. La importancia de medir los

procesos a través de indicadores de gestión contribuye a visualizar mejor el cumplimiento o no de los procedimientos.

3. Procedimientos de control asociados de negocio:

3.1 El responsable del área de seguridad es parte activa y fundamental del proceso de Seguridad en la Cadena de suministro Internacional y como tal debe estar actualizado en materia de los procesos que se llevan a cabo dentro de la organización en cuanto a los procesos de Importación y Exportación. Seguridad es uno de los factores claves en el éxito del control de riesgos y mitigación de los impactos y debe ser involucrado en todos y cada uno de los proyectos asociados a la Operación logística.

3.2 De manera estrecha se debe trabajar con el equipo para poder identificar los controles que se deben llevar a cabo para evitar la "infiltración" de personas o compañías que puedan tener contacto u operaciones asociadas al lavado de activos o financiación del terrorismo.

3.3 Los cargos críticos no pueden perder visibilidad y se deben seguir los pasos que se han diseñado para la selección, control y contratación de los mismos, siempre teniendo en cuenta que deben ser firmados los Acuerdos de responsabilidad para poder asegurar lo concerniente a la responsabilidad legal por la toma de decisiones.

3.4 Las visitas a los Asociados de negocio que van a hacer parte de la operación logística para evaluar que realmente cumplen con los mínimos requeridos de seguridad y que pueden hacer parte de los proponentes en caso de ser abierta una licitación para un servicio nuevo o adicional.

3.5 Es también necesario, que a los Asociados de negocio que sigan haciendo parte de la operación, se les haga su visita cada dos años, para

poder evaluar sí siguen cumpliendo con esos requisitos mínimos de seguridad y, además, ver cómo ha sido su nivel de servicio para realizar los ajustes en cuanto a reducción de incidentes o novedades.

3.6 Revisar de forma mensual con el área de seguridad las novedades ocurridas para poder diseñar planes de acción de acuerdo con lo revisado en los indicadores de gestión.

4. Líder de OEA y su rol con la seguridad en la cadena de suministro internacional:

4.1 Se obtiene la certificación y es probable que por decisiones de la organización ese Comité que fue creado para trabajar en la certificación se desintegre, eso puede pasar; lo que no puede ocurrir es que el proceso quede acéfalo, sin un dueño que lidere las reuniones de seguimiento que son necesarias para poder garantizar que todo el trabajo que realizó el equipo se pierda y quede sin control, sin gestión y sin validaciones.

4.2 Es entendible que tener una sola persona dedicada a este proceso puede ser considerado inviable, sin embargo; por temas de reputación, legales, contractuales y de operación, esta persona es necesaria para poder validar que los compromisos adquiridos se están cumpliendo y que se pueda levantar la mano para poder corregir los incidentes o novedades que se presenten con cada una de las partes involucradas dentro del proceso de Seguridad de la Cadena de suministro internacional

4.3 Este líder, debe también estar atento a cumplir tareas asociadas a dar continuidad al proceso como los de:

4.3.1 Agendar las visitas para los nuevos asociados de negocio

4.3.2 Programar las visitas de control de los asociados de negocios existentes

4.3.3 Revisar los KPIs asociados a los procedimientos que se diseñaron para OEA

4.3.4 Programar las reuniones con el Comité de OEA, para validar el desempeño del programa de seguridad y poner en evidencia las novedades o incidentes ocurridos, para así poder diseñar, financiar e implementar los planes de acción que se requieran para cerrar la novedad o incidente

4.3.5 Estar atento al presupuesto asignado a OEA, ya que, en varios casos, pudo suceder que para mejorar las condiciones de seguridad en las instalaciones, fue necesario implementar controles, electrónicos, humanos, mixtos o mecánicos, que requieren una persona para que identifique los gastos o inversiones que se necesitan para los mantenimientos preventivos, correctivos, ajustes o incluso reclamación de garantías de ser necesario.

4.3.6 Este líder, debe tener un canal de comunicación directo con el responsable de logística para que le pueda dar a conocer cualquier situación que pueda poner en riesgo la seguridad de la cadena de suministro internacional y así evitar triangulación innecesaria que pueda comprometer la seguridad de las personas, las instalaciones y la operación.

5. Comité OEA:

5.1 Como el punto anterior, este comité debe seguir vigente ya que es el soporte para el Líder de OEA, ya que es el responsable de tramitar ante la alta gerencia las necesidades o novedades que se presentan y que puedan poner en riesgo la seguridad de la cadena de suministro.

5.2 Debe ser un actor activo permanente y estar atento a los reportes, novedades, informes y presentación de indicadores de gestión para que pueda hacer un

seguimiento mensual del desempeño de los equipos, de los procesos y también para resolver las necesidades presupuestales o de gestión que se requiera realizar, ya sea para mantener o mejorar las condiciones de seguridad en la cadena de suministro.

6. Procesos de inducción y reinducción:

6.1 Las organizaciones sufren cambios permanentes debido a múltiples variables y esto debe ser tenido en cuenta ya que de carecer de programas de entrenamiento o tenerlos y no llevarlos a cabo, se deja una puerta abierta para que las amenazas aprovechen el desconocimiento y generen incidentes de seguridad.

6.2 Muchas compañías alinearon sus procesos de inducción teniendo un ambiente diferente al de la pandemia, un claro ejemplo es que se visualiza en vídeos o imágenes, que se comparten los Protocolos o Procedimientos de seguridad, sin el uso de tapabocas o sin la implementación de las medidas de bioseguridad, y esto puede generar confusión y produce en las personas que los ven la sensación de que el programa de seguridad no es relevante para la organización.

6.3 Las personas que ingresan a la organización como parte de los nuevos equipos, deben recibir la información antes de ingresar a las operaciones para que conozcan de primera mano cómo lidiar con los hechos asociados a personas sospechosas, paquetes y actitudes sospechosos.

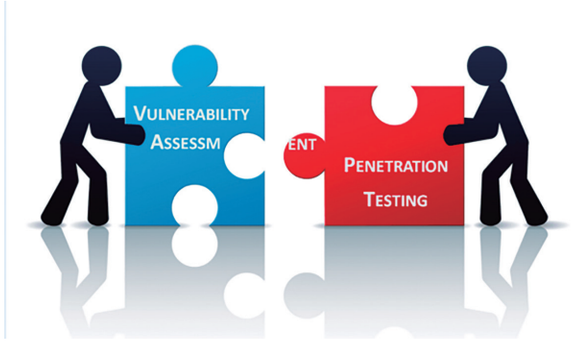
6.4 Este compromiso debe permear a toda la organización ya que hace parte de la Cultura de seguridad que se ajusta al programa de Conciencia de amenazas que se debe mantener activo y actualizado para reducir la

probabilidad de ocurrencia de incidentes o novedades de seguridad en la operación.

6.5 A pesar de haber realizado ya un proceso de entrenamiento es importante que por lo menos una vez al año, todos los colaboradores, asociados de negocio; reciban una reinducción para que tengan presente y pongan en práctica las medidas de seguridad que se han implementado para Proteger la Seguridad en la cadena de suministro internacional.

7. Pruebas de penetración o vulnerabilidad:

7.1 Un proceso, protocolo o procedimiento puede estar muy bien diseñado en el papel, sin embargo; cuando este no se pone a prueba no se va a conocer el resultado en un ambiente controlado, se va a ver es sobre el impacto de un riesgo que se materializó con los inconvenientes que esto puede llegar a tener (pérdidas totales o parciales, daños totales o parciales, interrupciones en las operaciones temporales o permanentes, entre otros).



7.2 Por eso es importante realizar las pruebas de vulnerabilidad o penetración, para poder identificar si las personas de la organización ponen en práctica lo que se les ha compartido a través de los entrenamientos y poder determinar cuáles son las oportunidades de mejora para así diseñar e implementar un plan de acción que permita mejorar las condiciones de las contramedidas de seguridad con las que se cuentan.

7.3 Diseñar e implementar un cronograma de pruebas de vulnerabilidad, que permita realizar al menos tres ejercicios al año, con diferentes escenarios que pueden estar incluidos en la matriz de riesgo.

7.4 Es importante tener en cuenta que para realizar este tipo de ejercicios se debe hacer en un espacio controlado, contemplar todas las variables

que se puedan salir de control, sólo avisar a quienes deben estar enterados y utilizar las herramientas que se necesiten para poder mantener el control del ejercicio.

7.5 Se pueden utilizar matrices de medición como la que se comparte en este ejemplo o las que el lector conozca o considere adecuada para su operación:

MATRIZ DE IDENTIFICACIÓN DE VULNERABILIDAD DE LOS SISTEMAS DE RESPUESTA

CONTRAMEDIDA	ACCIÓN REALIZADA	TIEMPO QUE LE TOMA AL INTRUSO (Minutos)	TIEMPO DE ACTIVACION DEL SISTEMA (Minutos)	ACCIÓN HUMANA DE SEGURIDAD	TIEMPO TOMADO (Minutos)	TIEMPO TOTAL DE LA RESPUESTA (Minutos)	NIVEL DE VULNERABILIDAD
Barrera Perimetrica de 8 pies sólida						0	0
Barrera Perimetrica 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

8. Procesos de control interno y compliance:

8.1 En este aspecto el *"Due Dilligence"* o Debida diligencia, sigue siendo relevante ya que los procesos asociados a SIPLAFT, SAGRILAFT, SARLAFT, se deben seguir realizando como desde el inicio del proceso de certificación. Es decir; se deben seguir validando todos los procesos de contratación en cuanto a personas y servicios para garantizar que no tienen ningún tipo de vinculo con organizaciones vinculadas a operaciones de terrorismo o narcotráfico.

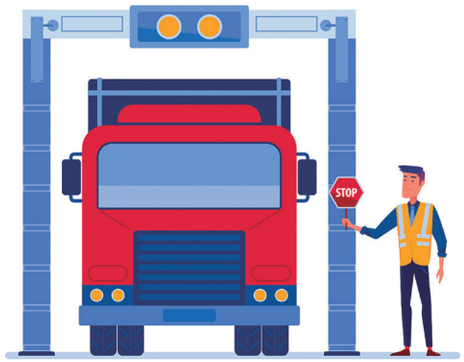
8.2 El *Controler* o quien haga sus veces debe estar informado y hacer parte de los comités o equipos que seleccionen y contraten los servicios para evitar la infiltración de personas u organizaciones que se conviertan en un factor de riesgo y que produzcan impactos directos o indirectos en los aspectos de reputación, legales u operacionales de las compañías.

8.3 El líder de este proceso de control, es responsable de estar recordándole al Comité de OEA o a los encargados de compras y contratos, la importancia de siempre revisar y validar la información de los oferentes o proponentes para que sea veraz, asociada al servicio que se requiere, que cumpla con los requerimientos escritos en la propuesta de servicio, que la documentación esté completa, que se realicen las visitas de asociado de negocio requeridas, que valide y verifique en los listados o programas para identificar sí pertenecen o no a organizaciones o personas que puedan o tengan vínculos con grupos terroristas o de narcotraficantes y poder dar aviso a la organización para suspender o no realizar procesos de contratación con esas entidades o personas.

8.4 Debe revisar en conjunto con el área legal, los términos del Contrato para establecer que en este quede inmerso todo lo relacionado con el servicio a prestar, las cláusulas de responsabilidad y de confidencialidad, así como las multas o sanciones por el incumplimiento de este.

9. Inspección de las unidades de carga:

9.1 Las unidades de carga siguen siendo uno los lados más vulnerables en la Seguridad de la cadena de suministro internacional, por varias razones, son manipulados, almacenados, reparados, usados por muchas personas o compañías y esto los deja expuestos a que sean previamente alterados para facilitar una contaminación en el proceso de cargue o descargue. Los procesos de inspección y selección deben ser acordes a las reglas de juego que se plantean en OEA, para reducir la probabilidad de que ocurran incidentes de seguridad que pongan en riesgo la operación y la reputación de una compañía.



9.2 A esto se le debe sumar, que una persona experta y preparada que tenga responsabilidad como Inspector de carga, debe seguir haciendo parte de los procesos y de la operación para así garantizar que la seguridad de las unidades de carga se siga cumpliendo y evitar que la carga, la reputación e incluso el cumplimiento a los clientes se puede ver comprometida.

9.3 Otro tema asociado a esto es que se hagan los reportes en tiempo y forma de todos los procesos que se siguen aguas arriba y aguas abajo, para notificar los cambios, novedades o incidentes que ocurran desde el origen y hasta el destino en cuanto a cambios de precintos, sellos, cambios del vehículo por cualquier tipo de novedad, cambio del conductor o retrasos generados por temas asociados a las vías, problemas de seguridad o imprevistos que se presenten.

Dentro de las novedades que se presentan continuamente está la de los precintos y algunos quizá asumen el riesgo que esto conlleva, sin embargo; una buena práctica es la de no aceptar el contenedor hasta que las navieras o compañías de logística aclaren la situación. Hay que tener en cuenta que esto no sólo afecta la seguridad de la cadena de suministro, sino que, también genera retrasos, problemas en la operación por desabasto de materias primas o producto terminado, sobrecostos por el incumplimiento en la devolución del contenedor y revisando un poco más profundo, los costos para el transportador por temas de gasolina, parqueaderos y por tener el vehículo sin producir o generar ingresos.

En cuanto a los riesgos asociados la seguridad de la cadena de suministro internacional, se encuentran:

- Riesgo de hurtos totales o parciales derivado de los movimientos adicionales que surgen cuando se identifica algo anómalo, extraño o sospechoso
- Riesgo de daños por temas asociados a accidentes de tránsito, debido a los movimientos adicionales y no programados
- Riesgo de contaminación, ya que el conductor se ve obligado a dejar el vehículo en sitios que quizá no cuenten con la suficiente seguridad
- Riesgo de ser retenido el producto en retenes de la Policía en alguno de los puntos de control que puedan estar operando en el lugar en el que se presentó la novedad

Teniendo en cuenta lo anterior, se pueden dar cuenta que este punto es muy importante ya que puede afectar de manera directa la seguridad y los procesos de una compañía.

10. Controles en la contratación de personal:

Se deben enfocar en los procesos de Selección, Reclutamiento y Contratación en los Cargos críticos que fueron identificados dentro del proceso de presentación de la compañía a OEA, se debe seguir manteniendo para evitar que se generen prácticas de corrupción que pueden afectar la seguridad de la cadena de suministro, se debe seguir ciñendo a los procesos de contratación. Por ello es importante determinar qué tipo de controles se deben seguir teniendo para reducir la probabilidad del ingreso de personas que pueden ser un riesgo para la compañía, la operación y la reputación de una compañía. Importante que se sigan manteniendo controles como:

- Revisión de toda la documentación presentada por el aspirante para validar su autenticidad, visita domiciliaria, presentación de su patrimonio (declaración de renta), certificaciones bancarias, certificaciones laborales (verificadas una a una), visita al vecindario para poder evaluar su comportamiento social, solicitud de antecedentes judiciales, de la Procuraduría y la Contraloría.

Además, cuando el candidato ha sido contratado, recuerden la importancia de hacerle firmar el acuerdo de RESPONSABILIDAD, para que quede amarrado a su proceso de toma de decisiones y se evite así que su cargo se preste para llevar a cabo acciones tendientes al Lavado de activos y Financiación del terrorismo.

Cuando se obtuvo la certificación OEA, muchos relajaron su nivel de estrés y eso está bien, sin embargo; es importante tener en cuenta que ser OEA, tiene muchas implicaciones que de perderse el control podrían poner en riesgo la continuidad de un negocio, es por ello, que se deben revisar y seguir aplicando juiciosamente todas y cada una de las recomendaciones sugeridas, con el fin de reducir la probabilidad de materialización de los riesgos que pueden afectar la Seguridad de la cadena de suministro internacional.

La certificación OEA, se pone en riesgo cuando la organización descuida la gestión, cuando quita parcial o totalmente los recursos para que la seguridad en la cadena de suministro siga siendo segura, se deja de lado el hacer seguimiento a los reportes de incidentes de seguridad, no se mantiene un equipo responsable de la administración de los procesos asociados a la certificación y se quitan los apoyos financieros para el mantenimiento, implementación o actualización de las contramedidas de seguridad. Se cae en el error de "bajar la guardia", creyendo que lo que hay no requiere de soporte, atención, gestión, actualizaciones o mantenimiento y olvidando que las amenazas siguen latentes y que pueden materializar los riesgos sí se lleva a cero o es nulo el seguimiento al Programa que se diseñó para obtener la tan necesaria y anhelada certificación.

La invitación aquí es la de poder generar un plan de seguimiento adecuado que contribuya con el mantenimiento de la certificación OEA, pero más allá de esto que siga contribuyen con el programa que se diseño para poder garantizar la Seguridad en la Cadena de Suministro Internacional.

CAPÍTULO 4

CÓMO GESTIONAR EL CONFLICTO DE INTERESES DESDE LOS VALORES ÉTICOS

Por: Ingeniero John Jairo Mónoga G.
Consultor y auditor para el Sistema de Gestión Antisoborno ISO 37001

La globalización y las estrategias de crecimiento empresarial de las organizaciones, han desarrollado nuevas oportunidades para que las empresas se concentren en sus verdaderas competencias y en su eficiencia operacional, motivando a generar una búsqueda de acuerdos o alianzas.

Según Peter Drucker, "la nueva fuerza integrante de la economía mundial son las alianzas a través de las fronteras. Las alianzas son la forma dominante de integración económica en la economía mundial. Una alianza crea una relación de sistemas con la que se establece una serie de redes de cooperación a fin de contribuir a la consolidación recíproca en el mercado internacional, ámbito donde ninguna organización puede permanecer sin la cooperación de otra"

Al efectuar estas alianzas, se comparten los costos fijos y los riesgos, e igualmente permite la transferencia de competencias o habilidades complementarias, así como la combinación de recursos para satisfacer intereses mutuos dando como resultado el fortalecimiento de la competitividad.

En ese sentido, las alianzas se deben desarrollar en un ambiente de confianza, transparencia e integridad con el fin de mantener una lealtad y fidelidad empresarial.

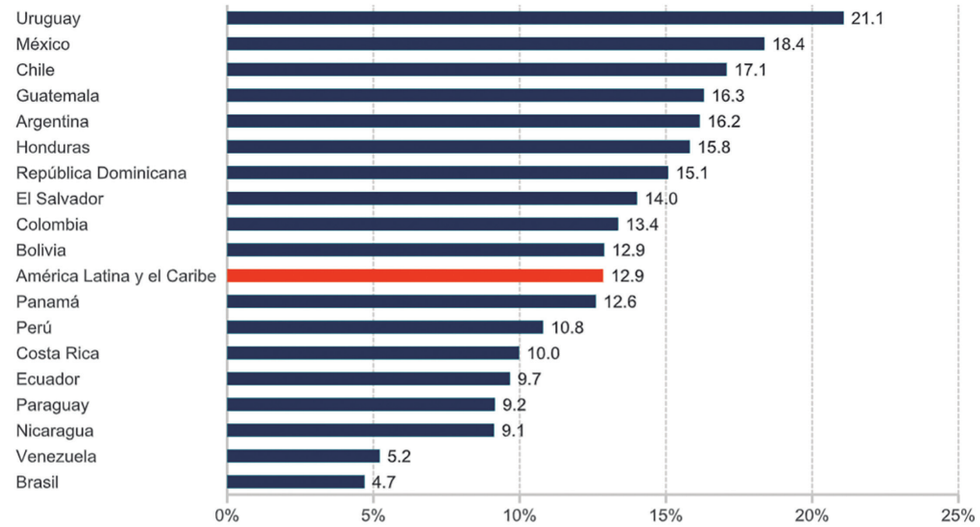
De acuerdo con el Banco Interamericano de Desarrollo, BID en la publicación "Confianza, la clave de la cohesión social y el crecimiento en América Latina y el Caribe" (1) indica : "La confianza es la creencia de que otros no actuarán de manera oportunista. No harán promesas que no pueden cumplir, no renegarán de las promesas que sí pueden cumplir ni transgredirán las normas para aprovecharse de otras personas que las respetan. En pocas palabras, la confianza es la fe en los demás: en su honestidad, fiabilidad y buena voluntad. Las personas confiables hacen promesas que pueden cumplir, no se desentienden de ellas y no transgreden las normas sociales"

Igualmente indica que "Nueve de cada diez personas en América Latina y el Caribe no creen que se puede confiar en los otros. Solo tres de cada diez confían en su gobierno y son incluso menos las que confían en las instituciones, fundamentales para la transparencia del gobierno, el Congreso y los partidos políticos"

Además, concluye que "Los países con mayor confianza tienden a gozar de mayores niveles de productividad, mientras que aquellos donde los índices de confianza son bajos, poseen una economía informal más grande en relación con su PIB".

En la siguiente gráfica se indica el "porcentaje de la población que confía en la mayoría de las personas", en donde América Latina y El Caribe tiene un 12.9% de confianza.

LOS NIVELES DE CONFIANZA EN AMÉRICA LATINA Y EL CARIBE SON REDUCIDOS



Porcentaje de la población que confía en la mayoría de las personas

Fuente: Keefer y Scartascini (2021).

(1) Fuente: https://publications.iadb.org/publications/spanish/document/Confianza-la-clave-de-la-cohesion-social-y-el-crecimiento-en-America-Latina-y-el-Caribe-Resumen-ejecutivo.pdf

Finalmente indica que: “Mayor confianza significa menos burocracia que daña a los negocios, a las inversiones y a la innovación. Significa gobiernos más transparentes, comprometidos en cumplir sus promesas y a rendir cuentas. Y, por último, también implica ciudadanos comprometidos que den voz a sus opiniones y participen activamente para realzar las democracias y apoyar la construcción de sociedades más inclusivas”

En ese sentido, las instituciones públicas y las organizaciones privadas requieren fortalecer su cultura, partiendo desde la integridad y la transparencia en cada una de sus actuaciones y actividades que realiza.

Se requiere una participación activa de los servidores públicos, los colaboradores, contratistas, trabajadores *in-house*, asesores, *freelance* y demás roles existentes para que esa cultura de integridad y transparencia sea una realidad.

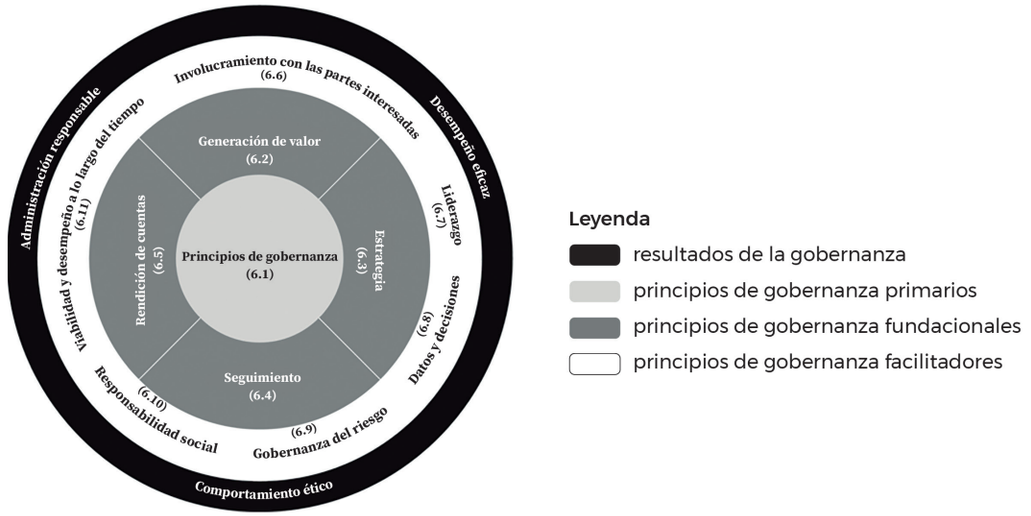
Por lo anterior, los conceptos de gobernanza, sostenibilidad, gobierno corporativo, cumplimiento y rendición de cuentas han tomado un protagonismo en las instituciones del estado y las organizaciones privadas.

La norma **ISO 37000:2021**, sirve como apoyo para que las organizaciones tengan unas directrices en materia de **gobernanza.** La ISO 37000 es sinónimo de confianza dado que la organización es responsable, rinde cuentas, es justa y transparente, y actúa con integridad y toma decisiones basada en el riesgo, soportada con información creíble y datos fiables.

La gobernanza se basa en el espíritu, la cultura, las normas, las prácticas, los comportamientos, las estructuras y los procesos de la organización.

Los principios primarios aseguran que la razón de ser de la compañía esté claramente definida, con relación al ambiente natural, la sociedad, y sus partes interesadas.

La siguiente figura describe los principios de la gobernanza que tiene como objetivo un desempeño eficaz, una administración responsable y un comportamiento ético.



Fuente de la imagen GTC-ISO 37000:2021 – ICONTEC

Los principios funcionales son la esencia para asegurar la eficacia en la gobernanza, ya que se definen los objetivos de generación de valor, las estrategias organizacionales, el seguimiento al desempeño y la rendición de cuentas.

Los principios facilitadores abordan las responsabilidades de la gobernanza en la organización, involucrando a las partes interesadas, con un liderazgo ético, reconociendo los datos como un recurso importante para la toma de decisiones, considerando el efecto de la incertidumbre sobre el propósito organizacional, asegurando que las decisiones sean transparentes y buscando la viabilidad y el desempeño a lo largo del tiempo.

El **gobierno corporativo** es el conjunto de normas, principios y procedimientos que regulan la estructura y el funcionamiento de los órganos de gobierno de una empresa. Establece las relaciones entre la junta directiva, el consejo de administración, los accionistas y el resto de partes interesadas para estipular las reglas por las que se rige el proceso de toma de decisiones de una organización.

Por ello, actualmente la firma *Ethisphere* realiza una evaluación para medir los estándares corporativos relacionados con la ética empresarial. El sistema de evaluación aplicado, está conformado por 200 preguntas relacionadas con el Programa de Ética y Cumplimiento, Cultura de Ética, Responsabilidad y Ciudadanía Corporativa, Gobernanza y Liderazgo y Reputación de una organización.

Cada categoría se evalúa a través de una combinación de respuestas a nuestro cuestionario *Ethics Quotient® (EQ)*, documentación complementaria enviada y, cuando sea necesario, investigación independiente y seguimiento. La evaluación de la categoría Liderazgo y reputación también incluye una revisión de la información disponible públicamente relacionada con la reputación de una organización por actuar éticamente (por ejemplo, presentaciones públicas, actividad regulatoria, revisión de los medios).

Para el año 2022, fueron galardonadas 136 organizaciones ubicados en 22 países y 45 sectores; de los cuales hay 14 que son galardonados por primera vez y 6 organizaciones que han sido nombradas en la lista de galardonados 16 veces. (fuente: https://ethisphere.com/what-we-do/worlds-most-ethical-companies/)

La cultura de la integridad se ve opacada cuando las instituciones y organizaciones no gestionan y previenen los conflictos de intereses, el tráfico de influencia, los actos indebidos, las preferencias, la corrupción, el soborno y otras actividades, las cuales generan una pérdida de confianza y credibilidad afectando la imagen y la reputación.

Se requiere prevenir que el interés particular interfiera o afecte las actividades y toma de decisiones de las instituciones y las organizaciones y así no incurrir en actividades que atenten contra la transparencia y la moralidad.

El conflicto de intereses surge cuando un funcionario público o colaborador tiene un interés privado que podría influir, o en efecto influye, en el desempeño imparcial y objetivo de sus funciones asignadas, dado que le resulta particularmente conveniente a él, o a su familia, o a sus socios cercanos.

Los conflictos de intereses ponen en riesgo la obligación de garantizar el interés general de un funcionario público o un colaborador de una organización afectando la confianza de las partes interesadas.

De acuerdo con la función pública en Colombia, el conflicto de intereses tiene tres clasificaciones:

1. **Real**: Cuando el servidor ya se encuentra en una situación en la que debe tomar una decisión, pero, en el marco de esta, existe un interés particular que podría influir en sus obligaciones como servidor público. Por ello, se puede decir que este tipo de conflicto son riesgos actuales.[1]

2. **Potencial**: Cuando el servidor tiene un interés particular que podría influir en sus obligaciones como servidor público, pero aún no se encuentra en aquella situación en la que debe tomar una decisión. No obstante, esta situación podría producirse en el futuro.[1]

3. **Aparente**: Cuando el servidor público no tiene un interés privado, pero alguien podría llegar a concluir, aunque sea de manera tentativa, que sí lo tiene. Una forma práctica de identificar si existe un conflicto de intereses aparente es porque el servidor puede ofrecer toda la información necesaria para demostrar que dicho conflicto no es ni real ni potencial.[1]

(1) fuente: https://www.funcionpublica.gov.co/documents/36031014/36151539/Guia-identificacion-declaracion-conflicto-intereses-sector-publico-colombiano.pdf/81207879-d5de-bec7-6a7e-8ac1882448c2?t=1572381672818#page=12)

Estas mismas situaciones se presentan en el sector privado, razón por la cual es necesario gestionarlas de manera preventiva con el fin de anticiparnos a su ocurrencia y de igual forma cómo abordarlos en caso que suceda.

Algunas actividades que permiten gestionar de manera preventiva el conflicto de intereses son las siguientes:

Actividades	Acción
1. Identificar los cargos y las actividades vulnerables al conflicto de intereses.	Revise detalladamente las responsabilidades, funciones y autoridad que tienen asignados todos los cargos Evalúe las decisiones que cada cargo toma en el desarrollo del cargo, e identifique aquellas que son estratégicas.
2. Elaborar una declaración en donde la persona manifieste potenciales conflicto de intereses.	Es muy importante que las personas que posiciones expuestas a conflicto de intereses, declaren su situación al momento de su vinculación y periódicamente, recomendable anualmente.
3. Realizar actividades de capacitación y toma de conciencia	Es necesario explicar y visualizar los potenciales escenarios de conflicto de intereses, con el fin de recrear estos eventos con ejemplos o casos prácticos, los cuales deben ser divulgados a través de capacitaciones, talleres, piezas de comunicación, entre otras

A continuación presentamos los elementos que debe tener la declaración de conflicto de intereses:

Declaración de conflicto o no conflicto de intereses	
Yo, _____ identificado _____ cargo _____ manifiesto conocer las actividades que originan conflicto de interés, inhabilidad o incompatibilidad y me comprometo a informar cualquier conflicto que a nivel personal llegue a comprometer o afectar a la institución o a la organización.	
Con la firma de este documentos, declaro que SI____ NO ____ me encuentro en una situación de conflicto de intereses real.	
En caso que la respuesta sea SI, por favor responder o ampliar la siguiente información: 1. ¿En qué consiste la causal del conflicto de intereses? 2. Explique la situación de conflicto de intereses aparente (no real ni potencial)	
Firma	Fecha y ciudad

CAPÍTULO 5

SEGUROS PARA LA CADENA DE SUMINISTRO Y SU APORTE A LA SEGURIDAD

Por: Reinaldo Andrés Rodríguez Guerrero.
Director General Grupo OET
(Administradores de Riesgos)

Resumen

Varios de los riesgos que afectan la cadena de suministro, pueden ser transferidos a terceros mediante el uso de seguros. Pero hoy en día, el papel de los seguros relacionados con la cadena de suministro va más allá de la transferencia de riesgo e involucra también el proceso de sensibilización y administración de riesgos dentro de los actores de la cadena de suministro, la generación de herramientas de control frente a riesgos concretos, y la difusión y gestión de información que permite identificarlos y gestionarlos de forma más eficiente.

En este artículo se exploran los distintos tipos de seguros existentes para proteger a la cadena de suministro frente a los riesgos a los que se ve expuesta, y cómo el sector asegurador, desde su visión experta en administración de riesgos, puede aportar a su seguridad de la cadena de suministro, como, por ejemplo:

1. Aporta a generar una cultura de administración de riesgos.
2. Brinda herramientas prácticas para el control de los riesgos.

Antecedentes

La cadena de suministro como toda actividad humana está expuesta a multiplicidad de riesgos. Durante la época de la colonia, las flotas españolas que transportaban el oro, plata y demás piedras preciosas que se extraían de las minas en América, o incluso otros productos como cacao y especias, estaban expuestas a un riesgo permanente. Los corsarios o piratas, hacían de las suyas y atacaban múltiples navíos para quedarse con la valiosa carga que éstos llevaban. Los españoles, tuvieron que implementar medidas de seguridad y crear convoyes para aumentar la seguridad del transporte, que incluía el uso de galeones fuertemente armados con cañones.

Este es un ejemplo de cómo desde siempre las actividades involucradas en la cadena de suministro, como en el caso anterior el transporte, han tenido una relación estrecha con la seguridad. La existencia de mayores o menores medidas de seguridad en la cadena de suministro que puede implicar, por lo tanto, una mayor o menor exposición y materialización de los riesgos que ésta enfrenta.

Ahora bien, los seguros, que constituyen una de las formas más extendidas de gestionar los riesgos mediante la transferencia financiera de los mismos a un

tercero, son muy sensibles a que existan medidas de prevención que lleven a una disminución en la probabilidad de su materialización. A las aseguradoras, les interesa de muchas maneras, que la siniestralidad de sus pólizas de seguros sea menor y, por lo tanto, les interesa promover con sus asegurados una cultura de prevención de riesgos donde la seguridad (que es uno de los mecanismos de prevención más efectivos) siempre debe estar presente.

Para las aseguradoras, la existencia de medidas o herramientas de seguridad se ha convertido en un elemento de prevención fundamental para las cadenas de suministro, y por lo tanto, en un elemento clave en la gestión de los riesgos que afectan a sus pólizas de seguros.

Los Riesgos en la Cadena de Suministro

El punto común que tienen la Cadena de Suministro y sus seguros, son los riesgos. Por una parte, y como ya lo indicamos, la cadena de suministro como toda actividad humana está expuesta a múltiples riesgos. En cuanto al seguro, éste encuentra su sentido en la ocurrencia del riesgo. Pero, para efectos prácticos, ¿qué entendemos por riesgo?

Existen múltiples definiciones de riesgo, algunas de ellas aplicadas en contextos específicos. Desde el punto de vista de los seguros y de la seguridad en general, el concepto de riesgo tiene una acepción negativa. Gabriel Verger lo define como “la incertidumbre que existe de que un hecho ocurra, durante un periodo y condiciones determinadas, comportando unas pérdidas económicas” (Verger, 1993).

El código de comercio colombiano por su parte, define el riesgo en su artículo 1054 como “el suceso incierto que no depende exclusivamente de la voluntad del tomador, del asegurado o del beneficiario, y cuya realización da origen a la obligación del asegurador”.

Ambas definiciones tienen en común la existencia de un hecho o suceso que es incierto o sobre el cual no se tiene certeza de su ocurrencia, y que tiene una consecuencia negativa, bien sea para el que lo sufre o en el caso del seguro, para el asegurador que deberá cumplir con la obligación de pagar una indemnización al asegurado por su ocurrencia.

Estos riesgos, es decir, estos hechos inciertos que cuando ocurren pueden generar una pérdida económica, se pueden manifestar en la cadena de suministro de múltiples maneras. Algunos ejemplos de los riesgos que pueden afectar a la cadena de suministro, son los siguientes:

1. Robo o hurto:

    1.1 De la carga.

    1.2 De los activos usados en las operaciones de la cadena de suministro (medios de transporte, dispositivos de control o seguimiento).

2. Accidentes ocurridos durante las operaciones propias de la cadena de suministro:

    2.1 Del medio de transporte (choque, volcamiento, varada).

    2.2 En operaciones de cargue o descargue de mercancías.

3. Incumplimiento de contratos.

4. Accidentes laborales o enfermedades profesionales.

5. Contaminación de las mercancías con narcóticos, armas o contrabando.

6. Guerras, huelgas, terrorismo.

La ocurrencia de los riesgos anteriores trae como consecuencia pérdidas económicas expresadas mediante:

1. Costo total o parcial de la carga o de los bienes dañados o perdidos.

2. Daños a la reputación de la empresa o marca.

3. Indemnizaciones por perjuicios causados a terceros.

4. Costos financieros.

5. Lucro cesante.

6. Multas o sanciones.

Este listado de riesgos y sus consecuencias, que no es exhaustivo, puede ser mucho más amplio y varía según las características de cada cadena de suministro. Así, por ejemplo, cuando hablamos de cadenas de suministro "especializadas" como las que manejan productos refrigerados, mercancías peligrosas o mercancías azarosas, pueden surgir otros riesgos propios del tipo de mercancía sobre la cual recaiga la operación de la cadena de suministro.

En el caso de productos refrigerados, la pérdida de la cadena de frio como consecuencia de un daño en el sistema de refrigeración (riesgo), puede generar el daño de la mercancía o su deterioro. Y este riesgo puede provenir de un mal mantenimiento del sistema de refrigeración, de un saboteo o descomposición de éste, por actos malintencionados de terceros.

Así mismo, es importante destacar que, la ocurrencia de un riesgo puede desencadenar otros riesgos y puede generar una o varias pérdidas económicas que afecten la cadena de suministro. Por ejemplo, el caso en el cual un camión que lleva bebidas se accidenta en carretera (riesgo de accidente), luego personas aledañas al lugar proceden a saquear la mercancía transportada por el camión (riesgos de robo).

Estos riesgos generan unas pérdidas económicas representadas en los lesiones e incapacidad del conductor (si éste sufrió daños en su integridad personal como consecuencia del accidente), daños en el camión o costos de su reparación, costos de las mercancías que fueron robadas y otros costos relacionados como el lucro cesante o pérdidas del mercado por no contar con los productos a tiempo en su lugar de destino.

Los Seguros en la Cadena de Suministro

La teoría nos indica que los riesgos pueden ser asumidos, gestionados, transferidos o evitados. Dentro de la categoría de transferencia de riesgos, éstos pueden ser transferidos financiera o contractualmente.

Una de las modalidades mediante la cual los riesgos pueden ser transferidos financieramente, se conoce como contrato de seguro. Es la figura más común mediante la cual las empresas o las personas pueden transferir sus riesgos.

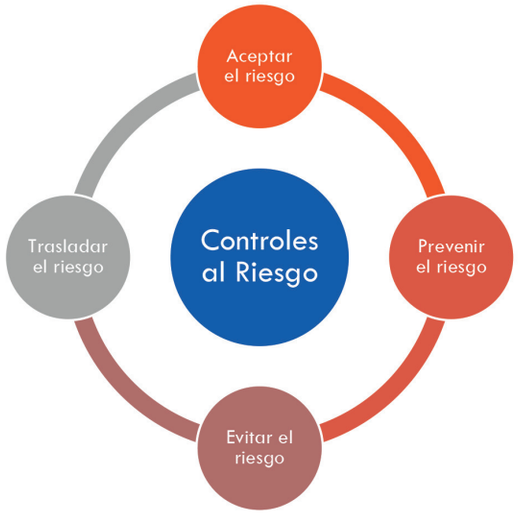


Figura 1. Controles que pueden ser implementados para el tratamiento de los Riesgos.

Mediante el contrato de seguro, una compañía de seguros asume los riesgos de una empresa o persona a cambio del pago de un precio, llamado prima. Es decir, una empresa o persona traslada las consecuencias del riesgo (las pérdidas económicas que pueda sufrir) a otra empresa, llamada asegurador, a cambio de una prima.

El Dr. Efrén Ossa, hace referencia a una definición de seguro de Joseph Hémard como "una operación por la cual una parte, el asegurado, se hace prometer, mediante una remuneración, la prima, para él o para un tercero, en caso de realización de un riesgo, una prestación por otra parte, el asegurador, que tomando a su cargo un conjunto de riesgos, los compensa conforme a leyes de la estadística" (Ossa Gómez, 1991).

El contrato de seguros tiene algunos elementos esenciales para su existencia. El código de comercio colombiano en su artículo 1045 establece "Son elementos esenciales del contrato de seguro: 1. El interés asegurable; 2. El riesgo asegurable; 3. La prima o precio del seguro, y 4. La obligación condicional del asegurador. En defecto de cualquiera de estos elementos, el contrato de seguro no producirá efecto alguno."

El interés asegurable hace referencia a la relación jurídico-económica entre el asegurado y el objeto a ser asegurado. Por ejemplo, cuando se asegura una carga frente a los riesgos de robo de ésta, debe existir alguna relación entre dicha carga y quien toma el seguro, quien asegura la carga debe tener un interés en que sobre la misma no recaiga el riesgo, ya que en caso de que éste ocurra, va a tener una pérdida económica que lo afecta directamente. En el caso de una compraventa internacional, por ejemplo, tiene interés asegurable el vendedor de una mercancía hasta cuando sea responsable de la entrega de ésta, según el término INCOTERM© que se haya pactado en dicha compraventa, o tendrá interés asegurable el comprador de ésta cuando según dicho INCOTERM© indique que él será responsable de los daños o pérdidas que pueda sufrir la mercancía.

El código de comercio define en su artículo 1083 "Tiene interés asegurable toda persona cuyo patrimonio pueda resultar afectado, directa o indirectamente, por la realización de un riesgo. Es asegurable todo interés que, además de lícito, sea susceptible de estimación en dinero".

El riesgo asegurable, que ya definimos en el capítulo anterior, se refiere a los que son asumidos por el asegurador y, que en caso de que se realicen, dan lugar a la obligación del asegurador de cumplir con una obligación, bien sea el pago de una indemnización en dinero o alguna otra que permita resarcir el daño sufrido por el asegurado.

La prima o precio del seguro hace referencia al valor que paga el asegurado o tomador del seguro al asegurador a cambio de transferir el riesgo. El seguro es una actividad comercial, las aseguradoras tienen un ánimo de lucro y buscan asumir dichos riesgos a cambio de un pago. Su negocio consiste en asumir muchos riesgos y distribuir la posibilidad de ocurrencia de éstos entre los muchos riesgos que son asumidos, aplicando lo que se conoce como la "ley de los grandes números", la cual "señala que si se lleva a cabo repetidas veces una misma prueba (por ejemplo, lanzar una moneda, tirar una ruleta, etc.), la

frecuencia con la que se repetirá un determinado suceso (que salga cara o sello, que salga el número 3 negro, etc.) se acercará a una constante. Esta será a su vez la probabilidad de que ocurra este evento." (Roldán, 2017). Dicha probabilidad permite al asegurador establecer cuándo tendrá que pagar por un riesgo y cuándo no, y a partir de allí, establecer a qué valor de prima podrá obtener una diferencia que será su ganancia.

Este modelo de negocio permite que riesgos que serían muy costosos asumir para una sola empresa o persona, sean distribuidos o compartidos con muchas otras empresas que pueden sufrir el mismo riesgo. La probabilidad de que a todos les ocurra el mismo riesgo, va disminuyendo si existe un número mayor de actividades en las cuales este riesgo puede ocurrir, sobre todo si el mismo está distribuido en diferentes ubicaciones geográficas, afecta a diferentes bienes o intereses o las actividades son realizadas por distintas empresas o personas. Por ejemplo, en el caso de la cadena de suministro, los riesgos se dispersan cuando se realizan operaciones en distintos países, cuando los productos que son objeto de los riesgos tienen diferente naturaleza y cuando los actores que intervienen en la cadena de suministro son distintos y variados.

El último de los elementos esenciales del seguro es la obligación condicional del asegurador. Ésta hace referencia a la obligación que surge para el asegurador cuando se ha realizado el riesgo. Es condicional, ya que surge cuando se materializa el riesgo, pero puede ocurrir que durante toda la existencia del seguro nunca se materialice el riesgo, por lo que la obligación no nacerá para el asegurador.

Dicha obligación puede consistir en el pago de una suma de dinero que compense el daño que ha sido causado por la materialización del riesgo. Por ejemplo, si la mercancía fue robada, se compensará el valor de ésta, o si ha sufrido una avería parcial se pagará el valor de dicho daño parcial. También puede consistir en la reposición del bien a nuevo o a un estado similar al que se encontraba antes de que se materializara el riesgo. Por ejemplo, si se materializa un daño del equipo de transporte porque el camión chocó a otro vehículo mientras realizaba el transporte, el asegurador podrá asumir la reparación del vehículo y dejarlo en el mismo estado en que estaba antes del choque, con lo cual cumpliría su obligación de reponer los bienes al estado en que se encontraban.

Algo importante para destacar, es que el seguro tiene como intención reponer los daños que ha sufrido el asegurado, no generar una riqueza para éste. En los

seguros de daños se aplica por regla general el principio indemnizatorio, según el cual "el asegurado no puede obtener del contrato de seguro sino la reparación del daño que efectivamente ha sufrido y en la medida real de ese daño, sin que puede pretender enriquecimiento de ninguna clase. El seguro está dirigido a reparar el daño sufrido por el asegurado de tal manera que éste vuelva a quedar en las condiciones en que se encontraba antes de que se sucediera el siniestro, pero no en mejores condiciones". (Ordoñez Ordoñez, 2001).

Se debe considerar que en la práctica no todos los riesgos pueden ser transferidos, por lo que no todos los riesgos que pueden afectar la cadena de suministro pueden ser objeto del contrato de seguros. Existen riesgos que deben ser asumidos por la empresa o tratados mediante controles para su prevención, algunos de ellos mediante medidas de seguridad física. Adicionalmente, y con el cambio y avance de las tecnologías y actividades económicas puede que por ciertos momentos no existan seguros para cubrir todos los riesgos que pueden afectar la cadena de suministro.

Ejemplos de riesgos que usualmente no se transfieren, tienen que ver con aquellos derivados de daños causados por actividades nucleares o radiactividad. Esta exclusión que manejan los seguros, tiene su razón de ser en que los daños causados por estas actividades pueden tener un impacto tan alto, que no existen primas que permitan cubrir los daños causados por estos riesgos. En general los riesgos catastróficos, que pueden tener un alto impacto o que pueden afectar un volumen muy alto de bienes o personas, están excluidos de las pólizas de seguros.

Los seguros para la cadena de suministro se pueden catalogar de forma similar a como se catalogan los riesgos a los que está expuesta la cadena de suministro. Podemos mencionar como principales seguros que pueden operar en la cadena de suministro, los siguientes:

1. Seguro de Transporte. Cubre los riesgos que puedan afectar a la carga objeto del transporte, de riesgos como daños a la misma por accidente del medio de transporte, robo o hurto de la mercancía, averías, saqueos, pérdida como producto de huelgas o guerra, entre otros riesgos. En general, cubre operaciones nacionales e internacionales en distintos modos de transporte (marítimo, terrestre, aéreo etc.) y en general todo tipo de mercancías. Las coberturas, condiciones y exclusiones dependen del tipo de operación realizada, mercancía a ser asegurada, sitios de operación, entre otras variables del transporte.

2. Seguros de Responsabilidad Civil. Cubren los daños causados a terceros por los cuales sea responsable el asegurado. Estos seguros se catalogan en responsabilidad contractual (cuando el daño se origina en el incumplimiento de un contrato) o extracontractual (cuando no existe ninguna relación con el tercero afectado). Algunos de estos seguros son de carácter obligatorio, como los que deben tomar en Colombia las empresas que realizan transporte de mercancías peligrosas por carretera (Decreto 1609 de 2002).

3. Seguros que cubren los medios de transporte. Según el medio de transporte, existen pólizas de seguros que cubren los riesgos a los que se pueden ver expuestos dichos medios de transporte. Así, por ejemplo, el seguro de vehículos pesados o de carga, cubre los camiones o vehículos que se pueden utilizar durante la operación de transporte terrestre. También los que aseguran las aeronaves, los buques, o demás medios de transporte, cada uno con sus características, coberturas y exclusiones particulares, según la naturaleza de cada bien y su operación. Incluso hoy en día existen seguros para drones, los cuales se espera que cada vez tengan más participación en la actividad logística. Éstos normalmente se combinan con una cobertura de responsabilidad, dado que la actividad de conducción por su naturaleza peligrosa, puede dar lugar a daños causados a terceros durante la conducción u operación del medio de transporte.

4. Seguro de cumplimiento. Este seguro está orientado a garantizar el cumplimiento de una obligación contractual y/o legal. Por ejemplo, durante la ejecución de operaciones de comercio exterior donde es necesario brindar ciertas garantías a la autoridad aduanera sobre la disposición de las mercancías que son objeto de disposiciones aduaneras especiales, este tipo de seguros sirven como garantía frente a la entidad aduanera. En Colombia, la DIAN (Dirección de Impuestos y Aduanas Nacionales) exige a los usuarios aduaneros, depósitos aduaneros, comercializadoras internacionales y otros actores del comercio exterior este tipo de seguros. También permite garantizar el cumplimiento de un contrato entre privados, y es cada vez de uso común en operaciones logísticas, exigir este tipo de seguro a los contratistas o asociados de negocios.

5. Seguros de Propiedades. Cubre los daños que puedan sufrir instalaciones físicas como edificios, bodegas, oficinas y en general cualquier tipo de

construcción y sus contenidos como equipos, mercancías o materia primas, muebles, entre otros. Usualmente la cobertura básica es por incendio o impacto de rayo, y se complementa con coberturas como explosión, daños por agua, anegación, avalancha, deslizamiento, terremoto, entre otros. La extensión de coberturas de este tipo de seguros puede ser bastante amplia y depende en gran parte de la ubicación geográfica del bien y su contexto.

6.Seguros de maquinaria y equipo. Durante las operaciones logísticas y de la cadena de suministro, es posible que además de los medios de transporte, se haga uso de máquinas o equipos especializados como montacargas, rotuladores, bandas transportadoras, lectores, impresoras o equipo de otras características. Todos estos equipos y maquinaria pueden ser asegurados frente a los riesgos que se puedan presentar durante su operación.

7. Seguros para Riesgos Laborales. Las personas que ejecutan las operaciones en la cadena de suministro no están exentas de sufrir riesgos durante sus actividades. Los seguros de riesgos laborales cubren daños causados por accidentes laborales o enfermedades profesionales que puedan ocurrir a los trabajadores. En Colombia, todo trabajador debe estar vinculado a una ARL (Administradora de Riesgos Laborales) que es una aseguradora de los trabajadores frente a los riesgos antes mencionados.

8. SOAT. Seguro Obligatorio de Accidentes de Tránsito. Como su nombre lo indica, este seguro obligatorio cubre los daños causados a las personas como consecuencia de un accidente de tránsito. Al tener la cadena de suministro, por lo general, un componente importante de transporte por vía terrestre, bien sea para el transporte o distribución de los productos, es un seguro que siempre se debe tener presente en toda operación logística. En otros países de Latinoamérica existen seguros obligatorios similares al SOAT, que también son de carácter obligatorio y cubren los daños causados como consecuencia de accidentes de tránsito.

9. Seguros de riesgos cibernéticos. Los procesos de digitalización e implementación de nuevas tecnologías que se han dado de manera cada vez más rápida en el mundo, han llevado a las empresas a implementar de forma masiva sistemas de información que faciliten su operación y su interacción con sus clientes. Las cadenas de suministro no son ajenas a este fenómeno y cada vez han implementado tecnologías que facilitan

en flujo de información, sobre todo en un negocio donde la integración y disponibilidad de información son claves. Esto ha generado también nuevos riesgos, derivados de la filtración de los datos, la vulneración de los sistemas de información o la no disponibilidad de éstos. Casos como los que han ocurrido en años recientes a varias líneas navieras que impidieron a sus clientes acceder a sus sistemas de información, y por lo tanto, programar y conocer el estado de sus embarques, que derivó en demoras en la entrega y desembarque de la carga, son solo algunos ejemplos de cómo este riesgo estará cada vez más presente en las operaciones de la cadena de suministro.

El listado anterior no es exhaustivo y existen muchos tipos de seguros que pueden operar para la cadena de suministro, algunos de los cuales son variaciones o combinaciones de los ya mencionados. Los seguros al igual que los riesgos están en permanente evolución, por lo que siempre es importante revisar en las matrices de riesgos de la cadena de suministro, cuáles riesgos nuevos pueden estar presentes y si existen soluciones de seguro que puedan apoyar su gestión.

Partes que intervienen en los Seguro para la Cadena de Suministro

Para el caso de la cadena de suministro, quien transfiere el seguro puede ser cualquiera de los actores de la cadena: Quien produce una mercancía y requiere enviarla a su cliente, o quien la compra y requiere recibirla en su fábrica o domicilio, quien la comercializa y quiere distribuirla, el encargado del transporte bien sea por vía marítima, terrestre o cualquier otro modo de transporte, quien realiza los procesos de almacenamiento, empaque, embalaje, quien la manipula en los procesos realizados durante el puertos, aeropuertos o sitios de cargue o descargue de la mercancía.

La mayoría de las legislaciones identifica dos partes dentro del contrato de seguros: el tomador y el asegurador. El artículo 1037 del código de civil colombiano establece: “Son partes del contrato de seguro: 1. El asegurador, o sea la persona jurídica que asume los riesgos, debidamente autorizada para ello con arreglo a las leyes y reglamentos, y 2. El tomador, o sea la persona que, obrando por cuenta propia o ajena, traslada los riesgos”.

Dentro del seguro también se puede identificar otras dos partes que tienen relación con el seguro: el asegurado y el beneficiario.

El tomador del seguro es quien celebra el contrato de seguro a nombre propio o de terceros, y se hace responsable del pago de la prima. En algunos casos puedo ocurrir que el tomador no tenga un interés asegurable directo con el bien objeto del seguro, pero si desea trasladar los riesgos que pueda ocurrir a éste. Un ejemplo aplicable a la cadena de suministro que ocurre en Colombia, es la póliza de transporte de carga que toman algunos transportistas terrestres a nombre de sus clientes generadores de carga. El tomador de la póliza es el transportista terrestre, pero el asegurado es el generador de la carga (quien contrata el transporte) quien tiene un interés asegurable sobre la mercancía.

El asegurado es quien tiene un interés asegurable sobre el objeto del seguro. Lo relevante es que como lo indicamos en el acápite anterior, exista un interés asegurable entre el asegurado y el objeto del seguro. Quien tiene dicho interés asegurable se identifica para efectos del seguro como el asegurado. Normalmente en la cadena de suministro el asegurado se identifica como aquel cuya pérdida o daño del bien asegurado tiene una afectación económica.

Por ello, se identifica al propietario o consignatario de la mercancía como asegurado en las pólizas de transporte, o el propietario de las oficinas o bodegas donde se almacena la mercancía, al propietario de los medios de transporte, o quien tiene una relación laboral con los trabajadores que se puedan ver afectados por un accidente de trabajo o enfermedad laboral, solo por mencionar algunos ejemplos.

Otra parte que interviene en el contrato de seguro es el beneficiario, que se identifica como aquel que recibirá la compensación, pago o reposición del bien como consecuencia de la ocurrencia del riesgo. Atendiendo al principio de indemnización que se mencionó con anterioridad, el beneficiario en los seguros de daños debería ser aquel que debe recibir la indemnización por el perjuicio económico generado por la realización del riesgo. Por ejemplo, en las pólizas de responsabilidad civil extracontractual, el beneficiario es el tercero que se pude ver afectado por un daño generado por el asegurado, tercero que puede no tener ninguna relación previa ni con el tomador ni con el asegurado, y que incluso no se tenía identificado al momento de tomar el seguro.

Relación entre seguros y seguridad en la cadena de suministro

El objeto de los seguros es asumir las consecuencias de la realización de un

riesgo, pero dichos riesgos pueden ser además objeto de medidas de seguridad que ayuden a su prevención y a minimizar la posibilidad de su ocurrencia o su impacto. Por lo tanto, es la seguridad una de las principales acciones que se pueden implementar por parte de las empresas para controlar sus riesgos y que a las aseguradoras le debería interesar y promover en sus asegurados, ya que unos riesgos más controlados implican para éstas un menor pago de siniestros.

Pero, además, el uso de medidas de control es relevante para las opciones de la cadena de suministro como tal, y se ha convertido en un requisito comercial para los distintos actores de la cadena, donde "el uso de medidas de seguridad es, además, un requisito indispensable para la consecución de los contratos de compra-venta, transporte y aseguramiento de mercancías" (Safelink Agente de Seguros, 2021).

En el caso colombiano, durante la década de los años 90 y comienzos del este siglo, las aseguradoras venían presentando una alta siniestralidad, especialmente en las pólizas de transporte, debido sobre todo a altos niveles de robo de las mercancías, mucha de las cuales eran objeto de auto-robo, suplantación, gemeleo y piratería terrestre.

Las aseguradoras entendieron que era necesario aplicar medidas de administración y prevención de riesgos con sus asegurados, además de exigir dentro de sus pólizas de seguros de transporte garantías y condiciones especiales para sus operaciones. Fue así como se desarrollaron por parte de las aseguradoras, con acompañamiento de empresas de administración de riesgos especializadas en transporte, como Grupo OET, programas orientados a identificar, evaluar, calificar y gestionar los riesgos de la mano con sus asegurados.

Mediante esta actividad se identificaron varias medidas de seguridad a ser implementadas y ejecutadas por los asegurados, la mayoría de ellas orientadas al transporte terrestre, siendo esta modalidad la más afectada por los siniestros presentados. Algunas de las actividades que se comenzaron a exigir en las pólizas fueron:

1. Realizar procesos estrictos de selección de vehículos, conductores y propietarios de vehículos, sobre todo cuando la operación es realizada con vehículos tercerizados.

2. Verificar en centrales de riesgos los antecedentes de los vehículos, conductores y propietarios utilizados para la operación de transporte,

3. Crear planes de ruta y hacer seguimiento a los mismos, mediante puestos de control en carretera y seguimiento voz a voz a los conductores. (Se debe destacar qué para la época, el uso de dispositivos GPS no era muy común, por lo que mecanismos como el reporte en puestos de control era una alternativa efectiva para controlar las operaciones terrestres).

4. Contar con acompañantes o escoltas para mercancías de alto riesgo de robo o de alto valor.

Surgió también la necesidad de trabajar de la mano con las autoridades, para que los procesos de reacción frente a intentos de robo y la posterior investigación y judicialización de los responsables fuera efectiva, especialmente en los casos donde estos robos involucraban bandas delincuenciales con un alto nivel de organización.

Esta iniciativa se vio materializada con la creación del Frente de Seguridad Empresarial por parte de la Dirección de Investigación Criminal de la Policía Nacional, donde las empresas que hacían parte del sector asegurador, del sector transporte de carga y las autoridades podrían compartir sus experiencias, información sobre las modalidades de hurto que afectan a la operación de transporte y buenas prácticas a ser implementadas por las empresas para disminuir las posibilidades de afectación por las modalidades delictivas que afectaban al sector, especialmente la piratería terrestre. Es de destacar que fue FASECOLDA (Federación de Aseguradores Colombianos) uno de los principales impulsores para la creación del Frente de Seguridad Empresarial, proceso en el cual también participó Grupo OET.

Este es un ejemplo de cómo el seguro puede ser un catalizador hacia la implementación de buenas prácticas de seguridad hacia sus asegurados. Hoy en día varias de las compañías de seguros del mercado cuentan con Programas de Administración de Riesgos mediante los cuales brindan apoyo a sus asegurados para la identificación, evaluación y calificación de sus riesgos y la implementación de planes de mejora y buenas prácticas para hacer frente a los riesgos que las pueden afectar.

Las aseguradoras han entendido que apoyar a sus asegurados en la implementación de prácticas seguras en sus operaciones no solo disminuye su siniestralidad, sino que les permite fortalecer su oferta de valor al agregar herramientas para el control de los riesgos como el acceso a centrales de

riesgos, plataforma de monitoreo, selección y control, así como sensibilización y capacitación permanente.

En el año 2001 y como consecuencia de los atentados a las Torres Gemelas se aceleró a nivel mundial, la implementación de estándares de buenas prácticas a nivel mundial que facilitaran los procesos de intercambio comercial, con un enfoque en disminuir riesgos como el contrabando, tráfico de armas, tráfico de drogas, financiación del terrorismo y lavado de activos. Si bien ya existían antes de esta fecha iniciativas como BASC (Business Alliance for Secure Commerce), las exigencias cada vez mayores de las aduanas a nivel mundial aceleraron la adopción de estándares como el C-TPAT.

Todas estas buenas prácticas, estándares y normas comenzaron a impactar a toda la cadena de suministro, especialmente aquellas que hacían operaciones a nivel internacional. Poco a poco las cadenas de suministro empezaron a implementar estándares como ISO 28000 para la gestión de los riesgos de sus cadenas de suministro y hacerlo de forma armónica y organizada.

Más recientemente las aduanas a nivel mundial han venido unificando sus criterios para facilitar los procesos seguros en el comercio internacional bajo iniciativas como OEA (Operador Económico Autorizado), que establece unas prácticas mínimas a ser operadas por las empresas que hacen operaciones de comercio internacional y todos quienes intervienen en sus cadenas de suministro. La intención es que la administración de riesgos sea protagonista en las operaciones logísticas a nivel internacional.

La adopción de estos estándares y buenas prácticas debe ser de interés de las aseguradoras, quienes deben promover, difundir y apoyar a sus asegurados para su implementación. A través de sus programas de Administración y Prevención de Riesgos, las aseguradoras pueden ser facilitadoras de estos procesos.

Un asegurado que cuenta con procesos estandarizados y orientados hacia la seguridad de sus operaciones, puede disminuir de forma considerable la materialización de sus siniestros y aportar al objetivo común que persiguen la seguridad y los seguros: gestionar adecuadamente los riesgos.

Referencias

Verger, G. (1993). *El Risk Management.* Barcelona: Editorial Hispano Europea.

Roldán, P. N. (7 de Junio de 2017). *Ley de los grandes números.* Obtenido de Economipedia.com: https://economipedia.com/definiciones/ley-los-grandes-numeros.html

Ordoñez Ordoñez, A. E. (2001). El carácter indemnizatorio del Seguro de daños. *Revista de Derecho Privado Universidad Externado de Colombia.*

Ossa Gómez, J. E. (1991). *Teoría general del Seguro.* Bogotá: Editorial Temis.

Safelink Agente de Seguros. (2021). *El Seguro en el Transporte de Carga.* México: ALSUM Asociación Latinoamericana de Seguros Marítimos.

CAPÍTULO 6

TRANSVERSALIDAD Y CORRELACIÓN DE LAS NORMAS ISO EN LA CONTINUIDAD DE OPERACIONES EN CADENA DE SUMINISTRO

Por: Eduardo Hernández Ruiz, José Ángel Vidaña Meraz (†), Jorge Jaramillo Baena, Rosa María Jiménez Mendoza Y Mercedes Escudero Carmona del Consejo de Seguridad en Cadena de Suministro, en colaboración con: Zuly Gloria Pacheco Ruiz (presidente de la Comisión de enlace con la Guardia Nacional de México de CANACINTRA).

El hecho de que un proveedor no entregue los recursos a tiempo con la calidad y el costo acordados puede desencadenar una interrupción en las operaciones del negocio, debido a lo anterior, la organización deberá gestionar objetivos que pueden tornarse conflictivos, como es el caso de la reducción en costos de operación y tiempos de espera para obtener los insumos necesarios en los plazos previamente establecidos a la vez que gestiona la continuidad en las operaciones de su cadena de suministro. Toda organización necesita lograr un equilibrio entre cumplir con los objetivos del negocio a la vez que desarrolla medidas de continuidad adecuadas, para ello tendrá que desarrollar una estrategia conocida como SCBCMS (Supply Chain Business Continuity Management System ó Sistema de Gestión de la Continuidad del Negocio de la Cadena de Suministro) el cual tiene como objetivo desarrollar la capacidad organizacional para no interrumpir el flujo de los insumos necesarios para la producción y entrega de productos o servicios en el tiempo y en las condiciones acordadas.

Para comprender el SCBCMS necesitamos conocer algunos conceptos:

Concepto resiliencia organizacional

La resiliencia organizacional es la capacidad de adaptación de una organización en un entorno cambiante, para anticipar y responder a amenazas y oportunidades que surgen de cambios repentinos. Este principio adaptado a cada eslabón de una cadena de suministro le permitirá desarrollar:

1. Una mayor capacidad para anticipar y abordar riesgos y vulnerabilidades,

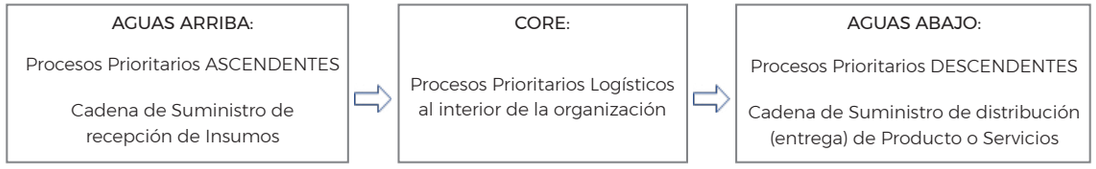
2. Una mayor comprensión de las partes interesadas y las dependencias que respaldan las metas y los objetivos estratégicos.

3. Una mayor coordinación entre los actores involucrados (socios comerciales -partes interesadas)

Concepto aguas arriba – aguas abajo

Las organizaciones dependen que los insumos sean entregados en tiempo y con la calidad previamente acordados. Esto se conoce como “AGUAS ARRIBA” o “procesos prioritarios ascendentes.

Las organizaciones también confían en poder entregar sus productos y servicios a sus clientes, ya sean en un siguiente eslabón de la cadena de suministro o bien, al cliente final. Todos los elementos considerados para cumplir con este objetivo, incluyendo el transporte, logística, servicios de tercerización, uso de tecnologías necesarias, etc. se conoce como “AGUAS ABAJO” o “procesos prioritarios descendentes.



Análisis de impacto al negocio (BIA)

El nivel de criticidad de proveedores y el tiempo de recuperación necesario, se determina durante la fase de ANÁLISIS DE IMPACTO AL NEGOCIO (BIA) Los proveedores prioritarios son aquellos que respaldan las actividades críticas de la organización y se identifican como aquellos que tienen el mayor nivel de impacto a la organización si no entregaran los recursos, lo cual afecta la capacidad de continuidad en las operaciones de la organización generando una incapacidad de entrega de productos y/o servicios.

Por definición, el análisis del impacto al negocio es la identificación de los activos críticos de negocio, funciones, procesos y recursos, así como una evaluación de los daños o la pérdida potencial que le puede causar a la organización como resultado de una interrupción (o un cambio en el entorno empresarial o de explotación). El análisis de impacto identifica cómo la pérdida o el daño se manifiesta; el grado del potencial de daño o pérdida con el tiempo después de un incidente; los servicios y recursos mínimos (humanos, físicos y financieros) necesarios para que los procesos de negocio continúen operando a un nivel mínimo aceptable y el plazo en el que las actividades, funciones y servicios de la organización deben ser recuperados.

BIA utiliza los siguientes valores:

MTD (MAXIMUN TOLERABLE DOWNTIME) o Tiempo Máximo de Inactividad

Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.

RTO (RECOVERY TIME OBJECTIVE) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

RPO (RECOVERY POINT OBJECTIVE) o Punto de Recuperación Objetivo. Hace referencia a un tiempo límite para que un servicio renueve su actividad. A partir del objetivo de tiempo que se marque la organización, tendrán que llevar a cabo ciertas tareas para garantizar el éxito.

WRT (WORK RECOVERY TIME) Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos

NOTA: Para conocer más acerca del BIA favor de referirse al artículo dentro de ésta guía denominado del autor Julián Andrés Puentes "Cómo establecer criterios para la continuidad de negocio en operaciones de cadena de suministro con BIA".

Concepto contexto interno y externo

El diseño e implementación de un marco de sistema de gestión se basa en una comprensión de la organización y su contexto de operación interna y externa. Por lo tanto, la organización debe definir y documentar su contexto interno y externo, incluida su cadena de suministro y subcontratistas. La organización debe evaluar los factores internos y externos que pueden influir en la forma en que la organización gestionará el riesgo.

Elementos que considerar en el desarrollo del CONTEXTO INTERNO:

1. Objetivos, estrategias y misión de la organización
2. Políticas para lograr los objetivos
3. Gobernanza, roles y responsabilidades
4. Estrategia general para la gestión del riesgo
5. Partes interesadas

6. Valores y cultura
7. Flujo de información y procesos de toma de decisiones
8. Actividades, funciones, servicios y productos
9. Marca y reputación
10. Uso del FODA

Elementos que considerar en el desarrollo del CONTEXTO EXTERNO:

1. El contexto cultural y político
2. El entorno legal, regulatorio, tecnológico, económico, natural y competitivo
3. Acuerdos contractuales, incluidas otras organizaciones dentro del alcance del contrato
4. Dependencias de infraestructura e interdependencias operativas con socios comerciales
5. Temas clave y tendencias que pueden impactar en los procesos y/u objetivos de la organización
6. Percepciones, valores, necesidades e intereses de las partes interesadas externas
7. Desarrollo del esquema de autogestión del COMPLIANCE
8. Uso del PESTEL

Concepto estructura iso de alto nivel (High Level Structure o HLS)

Se trata de una estructura dividida en 10 capítulos, que tiene como objetivo principal facilitar la integración de las normas de gestión de las normas ISO. Con esta estructura es más sencillo reunir diferentes normas ISO para desarrollar un sistema de gestión integrado.

En la siguiente imagen se correlaciona con las 4 etapas del PDCA:

OBJETIVO GENERAL DE CADA CLÁUSULA

CLÁUSULA 1: OBJETO Y CAMPO DE APLICACIÓN

Esta cláusula establece el objeto de la norma, así como los resultados esperados del sistema de gestión, los cuales deben ser específicos y coherentes con el contexto de la organización.

CLÁUSULA 2: REFERENCIAS NORMATIVAS

Proporciona detalles relevantes en relación con la norma de referencia.

CLÁUSULA 3: VOCABULARIO. TÉRMINOS Y DEFINICIONES

Detalla términos y definiciones aplicables a la norma de referencia.

CLÁUSULA 4: CONTEXTO DE LA ORGANIZACIÓN

Como punto de partida del sistema de gestión, esta cláusula debe identificar los aspectos internos y externos que puedan influir en los resultados esperados de la organización. Incluyendo la detección de necesidades de partes interesadas y/o grupos de interés a la vez que establece los límites del sistema de gestión alineados a los objetivos de la organización (modelo de negocio).

CLÁUSULA 5: CONTEXTO DE LA ORGANIZACIÓN

La alta dirección tiene ahora una mayor responsabilidad y participación en el sistema de gestión. Se integran los requisitos para lograr los resultados previstos asignando los recursos necesarios. La alta dirección es también responsable de comunicar la importancia del sistema de gestión aumentando la conciencia y participación de los empleados.

CLÁUSULA 6: PLANEACIÓN O PLANIFICACIÓN

Proporciona la manera de tratar el riesgo. Una vez que la organización ha definido riesgos y oportunidades en la cláusula 4 tiene que establecer cómo van a ser tratados, este enfoque proactivo reduce la necesidad de acciones correctivas futuras. Se presta especial atención a los objetivos del sistema de gestión. Nota: Es recomendable el uso de ISO 31000 e ISO 31010 en sus versiones más recientes.

CLÁUSULA 7: SOPORTE

Una vez abordado el contexto, el compromiso y la planeación, las organizaciones tendrán que analizar el soporte necesario. Esto incluye los recursos, comunicaciones internas y externas, así como la información documentada que reemplaza los términos utilizados anteriormente como documentos, documentación y registros.

CLÁUSULA 8: OPERACIÓN

La mayor parte de los requisitos del sistema de gestión se encuentra dentro de esta cláusula. También se abordan tanto los procesos internos como los

contratados externamente, mientras que la gestión del proceso global incluye criterios adecuados para el control de estos procesos, así como formas de gestionar el cambio planeado.

CLÁUSULA 9: EVALUACIÓN DEL DESEMPEÑO

Las organizaciones deben determinar qué, cómo y cuándo ha de ser supervisado, medido y evaluado el sistema.

La auditoría interna de primera y segunda parte aseguran que el sistema se ha implementado con éxito.

El último paso es la revisión por la dirección que analiza si el sistema de gestión es apropiado, adecuado y eficaz.

CLÁUSULA 10: OPERACIÓN

La última cláusula analiza cómo deben de tratarse las No Conformidades y acciones correctivas, así como las estrategias de mejora continua.

SCBCMS (SUPPLY CHAIN BUSINESS CONTINUITY MANAGEMENT SYSTEM O SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO DE LA CADENA DE SUMINISTRO

Las cadenas de suministro de las grandes organizaciones son cada vez más complejas y vulnerables, esta es la razón por la que es indispensable evaluar el rendimiento de proveedores ante diversos eventos tales como: desastres naturales, incidentes de falsificación, fraudes y otros factores que pueden dañar significativamente la continuidad en sus operaciones y por consiguiente afectarnos a nuestra propia operación. Por lo anterior se recomienda el desarrollo de un Sistema de Gestión en la Continuidad del Negocio de la Cadena de Suministro denominado por sus siglas SCBCMS *(Supply Chain Business Continuity Management System)*

SCBCMS ayuda a las grandes organizaciones a responder a dos preguntas clave relacionadas con los socios de la cadena de suministro de cualquier organización:

1 ¿Cuál es su capacidad real para enfrentar situaciones adversas en diferentes escalas y cual su capacidad para restablecer sus operaciones

en relativamente poco tiempo?

2 ¿Cuenta con un sistema homologado de continuidad de negocios conforme a normativas internacionales?

En el caso de que se responda sí a esta segunda pregunta, se deberá profundizar en el grado de madurez del SCBMS, por lo que podemos ampliar con las siguientes preguntas:

1. ¿Quién tiene la responsabilidad del programa de continuidad del negocio?

2. ¿Con qué frecuencia se actualizan sus planes de continuidad?

3. ¿Con qué frecuencia y mediante qué método(s) capacita a su organización en la continuidad del negocio?

4. ¿Cuenta con un comité de crisis y BCP?

5. ¿Cuándo ejecutó su última prueba de tecnología de continuidad del negocio?

6. ¿Tiene su organización un sitio de recuperación alternativo?

En diferentes sectores, por ejemplo, el automotriz se refieren a los proveedores por niveles, denominado Tier 1, Tier 2, etc.

El «Tier» define la relación del proveedor con la organización. Un proveedor crítico (Tier 1) tiene una relación directa con la organización, mientras que un proveedor indirecto (Tier 2) es el proveedor de nuestro proveedor y como tal, es más difícil de controlar por nuestra organización. Por lo que desarrollar un SCBCMS tanto en la propia organización como en los Tier 1 y Tier 2 mejorará la continuidad de toda la cadena de suministro. Sin embargo, existe mucha confusión cuando se pretender homologar criterios, esta es la razón por la que se ofrece una tabla sencilla de normas y estándares ISO que le ayudarán a crear un SCBCMS robusto y confiable haciendo la aclaratoria de que poco servirá si únicamente se implementa en la propia organización, pero no en los Tier 1 y Tier 2

Para desarrollar correctamente SCBCMS, la recomendación es implementar la nueva actualización de la ISO 28000 versión 2022.

¿Qué es ISO 28000:2022 y qué relación guarda con el SCBCMS?

La norma ISO 28000 originalmente fue publicada por ISO en el año 2007 denominado Sistema de Gestión de Seguridad en Cadena de Suministro y su actualización oficial fue publicada el día 15 de Marzo del 2022 presentando muchísimas mejoras respecto a la versión del 2007 de las cuales destacamos las siguientes:

a. Deja atrás el concepto limitado de gestión de la Seguridad en la cadena de suministro, ahora se incorpora el concepto RESILIENCIA en la Cadena de Suministro

b. Se crean 8 principios generales de aplicación (Liderazgo, Enfoque Estructurado, Personalizado, Compromiso Inclusivo de las Personas, Enfoque Integrado, Dinámico continuamente mejorado, Factores Humanos y Culturales y Gestión de las Relaciones) y

c. Esta nueva versión ya está alineada a la estructura ISO de alto nivel HLS, permitiendo así una integración perfecta con diferentes normas ISO HLS como es el caso de la ISO 31000, ISO 27001 y en especial, la ISO 22301:2019.

EL concepto de Resiliencia desde el estudio de la conducta humana es la adaptación a un entorno adverso de una persona, una vez superada esa adversidad podrá continuar con su plan de vida, pero ahora ha alcanzado en el proceso, un aprendizaje que le permitirá desarrollar una resistencia mayor ante próximos eventos similares, este concepto trasladado a cada eslabón de una cadena de suministro es precisamente el objetivo de la nueva versión de ISO 28000:2022

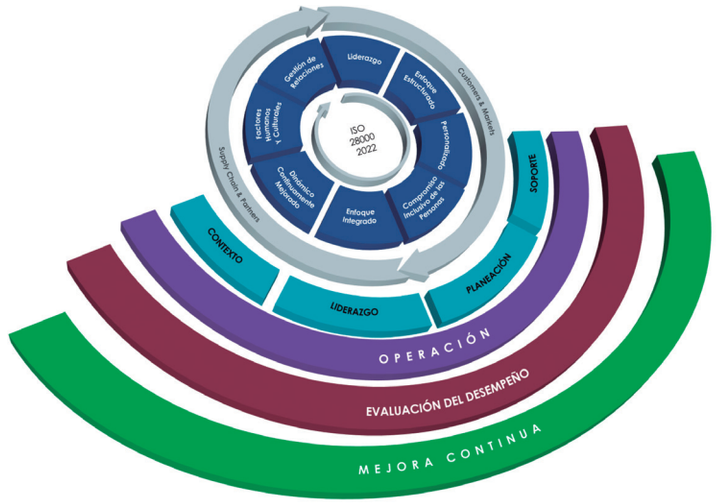


Imagen: Principios y Estructura de Alto Nivel de ISO 28000: 2022

Tres momentos para desarrollar en el SCBCMS

1. Antes del incidente

Antes de que ocurra una interrupción, la organización debe acordar lo siguiente con cada proveedor:

1.1 Puntos de activación y límite de tolerancia

1.2 Cómo activar los canales de comunicación previamente establecidos

1.3 Ejercitar y probar estrategias y soluciones de la cadena de suministro

2. Durante un incidente

Durante el incidente, la organización y los proveedores involucrados deben:

2.1. Activar canales de comunicación específicos de continuidad

2.2 Invocar y coordinar las estrategias y soluciones apropiadas

2.3 Monitorear la situación cambiante y las implicaciones para la continuidad de la organización

3. Después del incidente

Después del incidente, la organización debe realizar revisiones conjuntas. Tanto la organización como cada proveedor deben:

3.1 Producir y evaluar informes posteriores al incidente

3.2 Documentar las lecciones aprendidas, las áreas de mejora identificadas y las no conformidades

3.3 Documentar las acciones correctivas

3.4 Programar seguimientos para asegurar la implementación de acciones correctivas.

La necesidad de poner en práctica el BCMS

Ejemplos de ejercicios conjuntos con proveedores:

1. Ejercicio de simulación EN SITIO: Llevar a cabo ejercicios basados en escenarios para revisar el conocimiento de los participantes sobre las acciones requeridas en situaciones dinámicas específicas

2. Simulación A DISTANCIA: un ejercicio planificado basado en interrupciones específicas que requieren la implementación real de planes de recuperación.

A continuación, se presenta el listado de correlación de las normas ISO necesarias para el desarrollo integral del SCBCMS:

NORMA	OBJETO DE LA NORMA
ISO 22300:2021	Vocabulario de Seguridad, Resiliencia y BCM
ISO 22301:2019	Business Continuity Management System
ISO 22313:2020	Guía del uso del BCMS
ISO 22316:2017	Principios de Resiliencia Organizacional
ISO 22317:2021	Análisis de Impacto al negocio BIA
ISO 22318:2021	Continuidad de negocios en cadena de suministro
ISO/TS 22332:2021	Directrices para desarrollar planes y procedimientos de continuidad del negocio
ISO/DIS 22361	Gestión de Crisis (Norma en Desarrollo)
ISO 27001 (Familia)	Familia de normas de ISO 27001 seguridad de la información
ISO 28000:2022	Gestión de Seguridad y RESILIENCIA en Cadena de Suministro
ISO 28002:2011	Desarrollo de la RESILIENCIA en la cadena de suministro
ISO 30301:2019	Gestión Documental acorde a la Estructura de Alto Nivel HLS
ISO 31000:2018	Directrices para la gestión del riesgo
ISO 31010:2019	Técnicas de evaluación del riesgo
ISO 31073:2022	Vocabulario aplicable a la Gestión del Riesgo (Sustituye al Guide 73:2009)
ISO 37301:2021	Sistema de Gestión del Compliance
ISO 6346:2022	Contenedores de carga Codificación, identificación y marcado

CAPÍTULO 7

HERRAMIENTAS PARA DEMOSTRAR CONFIABILIDAD NTC ISO/IEC 27701:2020 TÉCNICAS DE SEGURIDAD. EXTENSIÓN A ISO/IEC 27001 E ISO/IEC 27002 PARA LA GESTIÓN DE LA PRIVACIDAD DE LA INFORMACIÓN. REQUISITOS Y DIRECTRICES.

Por: John Jairo Gutiérrez, Ingeniero Industrial.
Auditor de Sistemas de Gestión de ICONTEC

Confiabilidad, cualidad que debe ser demostrada por un sistema de gestión donde las miradas de las partes interesadas son amplias y detalladas, no es para menos por que los retos que impone la privacidad de la información son desafiantes y todas las entidades y empresas privadas deben diseñar mecanismos que brinden resultados eficaces, precisos y eficientes.

Se impone una necesidad que los sistemas de gestión deben presentar resultados confiables, sin embargo, se convierte en una tarea titánica la implementación de un nuevo estándar cuando en la organización se tiene implementadas varias normas, que, a pesar, que tiene toda la importancia del caso, los responsables deben atender prioridades y ser muy eficientes para que los procesos dimensionados brinden apoyo real y no se conviertan en cargas de tramitomanía, tan cuestionada.

Nuestra sociedad moderna tiene alta dependencia de la información electrónica y de los datos que colectamos de los usuarios, por eso se convierte en tarea fundamental poder demostrar adecuadamente mediante evidencia objetiva y rastreable para asegurar la adecuación y conformidad que se tiene frente al tratamiento y consentimiento de recolección, actualización, rectificaciones o revocatorias de la información personal y la conservación de su privacidad.

NTC ISO/IEC 27701:2020 es una norma muy especial ya que tiene un contenido con múltiples enfoques:

1. Estructura de alto nivel que desde hace años facilita la implementación sincronizada con otros estándares y facilita el desarrollo de herramientas comunes, aunque con despliegues particulares, tal es el caso de temas de construcción de la política, objetivos, revisión por la dirección, desarrollo de competencias, auditorias o acciones correctivas, entre otros

2. Capacitación, porque requiere de claridad en los conceptos que se aplican tanto del lado de los líderes de implementación como de los usuarios y responsables.

3. Inventario normativo, este es un trabajo multi - disciplinario ya que no solamente se precisa de saber la codificación de las normas aplicables sino la importancia de aplicarlas de forma precisa, a manera de ejemplo se identifican algunas normas, que conviene revisar de manera exhaustiva:

3.1. “Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)”, en línea con el artículo 26 y 27 del Decreto 1377 de 2013. Directriz que acoge los planteamientos formulados por la Organización para la Cooperación y el Desarrollo Económico (OCDE),

3.2 Ley 1581 de 2012 y decretos reglamentarios

3.3 El marco y los principios de privacidad diseñados en ISO / IEC 29100:2011 (ratificada en 2017) proporciona referencias a principios de privacidad conocidos para la tecnología de la información y define los principales actores y sus roles.

3.4 NTC ISO/IEC 27018:2020; Técnicas de seguridad. Código de práctica para la protección de la información de identificación personal (IIP) en las nubes públicas que actúan como procesadores de la IIP. Esta norma fue recientemente aprobada en comités técnicos de normalización de ICONTEC

3.5 ISO/IEC 29151 código de prácticas para la protección de información

4. Enfoque de Riesgos, más allá de la metodología escogida para su aplicación, ya sea ISO 31000:2018 Gestión de riesgos – directrices, o la ISO IEC 27005:2018 Gestión de riesgos de seguridad de la información u otras, es conveniente que se tenga un enfoque pragmático para hacer una identificación exhaustiva y precisa con el fin de no omitir planes que sean fundamentales, y es acá donde debe hacer un análisis holístico con los sistemas implementados para que los criterios tengan la capacidad de tomar en consideración situaciones relevantes para la gestión de la privacidad de la información. Tenga en cuenta que un tema es la metodología escogida (revise la norma ISO 31010:2019 Técnicas de gestión de riesgos, para identificar con precisión la metodología requerida) y otra, es la mecánica con la que se pueda aplicar, donde se pueden utilizar herramientas de ayuda tales como software de apoyo, pero considere que ambos temas son relevancia para los usuarios.

5. ISO IEC 27701 explora un concepto donde analiza los requerimientos de la estructura de alto nivel contenidos en ISO IEC 27001 (Requisitos), y su complemento, Anexo A (Controles, cuya guía práctica esta ilustrada

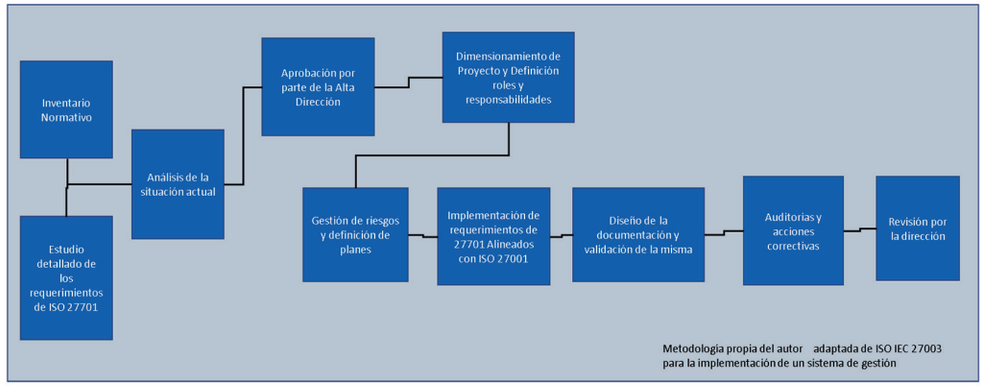
en ISO IEC 27002), para que se convierta en una extensión de seguridad de la información.

6. Al revisar los numerales 4.2, 4.3 y 5 de ISO IEC 27701 se muestra la manera de implementar como un par sincrónico el requisito de la norma de seguridad de la información y Los requisitos adicionales requeridos parala gestión de la privacidad.

7. Los anexos presentan una relación directa de los controles contenidos en las normas ISO 27001 e ISO 27002.

8. Respecto al punto anterior conviene considerar que ISO IEC 27002 acaba de tener una actualización de versión hacia 2022, sin embargo, su espíritu y fundamento son vigentes para los propósitos necesarios de implementación, se recomienda hacer una revisión exhaustiva de las normas nuevas para empezar el plan de alineación, junto con las instrucciones que brinde el Icontec para la transición de la certificación, el cual se brinda un tiempo prudencial.

9. Al implementar cualquier nuevo estándar, tal como ISO 27701, conviene considerar las recomendaciones de ISO IEC 27003:2017 Directrices para la implementación de un sistema de gestión de la seguridad de la información, se presenta a continuación un gráfico que podría explicar esas directrices



Es importante tener en cuenta:

1. Antes de arrancar a dimensionar controles, se debe tener una aprobación de la alta dirección para que se definan roles y recursos

2. La alta dirección toma una decisión con base en datos y planes consistentemente planeados basados en la situación actual y en el conocimiento pleno de las actividades a emprender

3. El diseño de la documentación toma en consideración la metodología de riesgos

4. La implementación de documentos debe validarse para asegurar su idoneidad

CAPÍTULO 8

CRITERIOS PARA GESTIONAR LA CONTINUIDAD DEL NEGOCIO EN OPERACIONES DE CADENA DE SUMINISTRO

Por: Julián Andrés Puentes B., CPP, PSP

Introducción

La continuidad de las operaciones ha tomado relevante importancia dados los efectos que su interrupción, han acumulado por cuenta de las restricciones en los momentos de confinamiento total que impuso la COVID-19; infortunadamente algunas las organizaciones han aprendido las bondades de la planificación de escenarios de gran impacto, desde el ejercicio negativo de la pérdida.

Esa imposibilidad de dar la continuidad en modo "normalidad" ha comprometido el interés del liderazgo ejecutivo ya que este, se centra en la supervivencia del negocio y la entrega de beneficios a sus partes interesadas, que al final no es más que la continuidad de negocio; sin embargo, los representantes de seguridad corporativa, muchas veces no comprenden que podría afectar esa supervivencia, no cuentan con criterios para establecer las necesidades de continuidad de negocio ya que en la mayoría de casos implementan modelos, que son exclusivamente de prevención (reducción de la probabilidad) y en algunos pocos casos, de mitigación (reducción de la consecuencia).

En ese sentido, la pretensión de este artículo es establecer la importancia de diseñar iniciativas con criterios prácticos, para atender la continuidad de negocio desde el establecimiento de las necesidades reales hasta las alternativas costo beneficio; para esto va a ser necesario conocer como los intereses de la organización se convierte en objetivos estratégicos como estos se desescalan para convertirlos en objetivos de la unidad de protección de activos; esto lleva al lector a inferir que se hace necesario establecer los términos en los que las diferentes actividades de la naturaleza del negocio se vuelven vitales en pro de la supervivencia de la organización, y de esta manera se entregan a las organizaciones oportunidades para medir los beneficios como la comparación entre la máxima perdida posible y la expectativa anual de perdida; de manera que una salida (o entregable) en el Análisis de Impacto en el Negocio (BIA por sus siglas en inglés) sea una efectiva decisión basada en la relación costo beneficio.

En ese sentido, la adopción e implementación sistemática de una serie de técnicas de gestión de la continuidad del negocio al interior de la organización, basadas en criterios objetivos ha contribuido a los resultados óptimos para todas las partes interesadas y más adelante afectadas. Ahora, las iniciativas de continuidad no se han diseñado para crear barreras comerciales, ni para aumentar o cambiar las obligaciones legales de una organización, como

tampoco crear actividades adicionales innecesarias, de hecho, la conformidad y la aceptación de las diversas no otorga, por sí misma, inmunidad frente a las obligaciones legales o la prevención de eventos disruptivos, indeseables y/o perturbadores.

El nivel de detalle y complejidad de las iniciativas, la amplitud de la documentación y los recursos que se han dedicado dependen de una serie de factores, tales como el ámbito de aplicación; el tamaño de la organización; y la naturaleza de sus actividades, productos y servicios, ya que los desastres naturales, los accidentes ambientales, los percances tecnológicos y las crisis provocadas por el hombre. De tal manera que históricamente, se evidencia que los eventos disruptivos van a suceder, y estos van a tener un impacto sobre los objetivos de la organización. El reto para las organizaciones va más allá de un mero plan de emergencia o de respuesta ante emergencias o de las actividades de gestión de desastres. Las organizaciones se deben involucrar en un proceso exhaustivo y sistemático para gestionar la continuidad de sus operaciones. Los riesgos actuales han requerido la creación de un proceso de gestión continuo, dinámico e interactivo basado en criterios determinantes que sirvan para asegurar la continuación de las actividades claves de la organización antes (resiliencia), durante (respuesta) y después (recuperación) de un incidente disruptivo grave.

Alineación estratégica

La gestión de los profesionales de seguridad, a todas luces es estratégica, aunque en el organigrama se vea táctica, esa transversalidad y su autoridad funcional, la vuelve estratégica; más cuando acompaña de manera decidida el cumplimiento de los propósitos organizacionales. Las organizaciones exitosas, acostumbrar a desarrollar anualmente ejercicios de planeación estratégica o de prospectiva estratégica que los ayuda a definir los objetivos organizacionales (estratégicos) que se pretenden cumplir para el año siguiente; de esta manera, la alta dirección, establece cuál es el propósito general y a partir de ahí, cada área funcional debe determinar sus propios objetivos (nivel táctico) y que se relacione con la estrategia, de tal manera que cada tarea desarrollada se convierte en un objetivo pero de tipo operativo. De acuerdo con lo anterior, la materialización de un riesgo operativo incrementa la probabilidad de materialización de un riesgo táctico y a su vez la materialización de este riesgo táctico aumenta la

materialización de un riesgo estratégico; razón por la cual, se interpreta como riesgo aquel obstáculo que pudiera impedir que se cumplan los objetivos en cada uno de los niveles (estratégico, táctico y operativo).

Ahora bien, en la identificación de los objetivos estratégicos se encuentra que la gran mayoría se asocian al negocio, a la continuidad de las operaciones, a la supervivencia de la organización, al incremento en ventas, al aumento en utilidades, a la penetración o participación ascendente de un mercado objetivo, en la penetración de nuevos nichos de mercado, entre otros. Dicho eso se puede identificar que es mucho más relevante para la organización, aquella área de seguridad que hace de sus prioridades, la continuidad de las operaciones, no solamente desde el segmento preventivo sino más aún hoy en día, en el segmento de mitigación.

Muchas de las prácticas en el mercado se están enfocando exclusivamente en modelos preventivos que contribuyen a la reducción de la probabilidad, pero muy pocas toman como base los procesos o los modelos de mitigación, donde se busca la reducción del impacto, modelos donde una vez materializado el evento, el área de seguridad se enfoca en la resiliencia organizacional, en la mitigación del incidente y en la recuperación de desastres como aquellos factores claves de una gestión de continuidad. De acuerdo con lo anterior, es importante establecer que, para conducir una efectiva evaluación de riesgos, se requiere determinar cuáles son los procesos críticos de la organización y por ende sus activos críticos toda vez que estos contribuyen al logro de los objetivos organizacionales, es decir que en la medida que el objetivo táctico protege el interés de la organización está contribuyendo al objetivo organizacional.

Establecimiento de criterios

Diferentes metodologías para establecer en realidad la importancia de los riesgos de la organización, ha acudido a una fórmula universal, a una fórmula estándar como es la probabilidad por la consecuencia, sin embargo, este tipo de modelos consuetudinariamente carecen de objetividad.

Diversas metodologías, a partir de modelos cuantitativos, han determinado unos factores para calcular la probabilidad más allá de la mera experiencia histórica y a su vez modelos que han permitido calcular la consecuencia aún más allá de la afectación económica, sin embargo es importante mencionar

que el modelo que se basa en una ecuación estándar está determinada por multiplicar la probabilidad por la consecuencia, lo cual, en esta expresión significaría de golpe asumir que ambas variables tienen la misma incidencia, es decir que un riesgo es 50% probabilidad y 50% consecuencia, mientras los diferentes estudios que sé que se relacionan en la referencia bibliográfica con la que ha sido construido este artículo, refiere que particularmente en estos tiempos pandémico o “pospandémicos”, la consecuencia es mucho más influyente, que la probabilidad, de hecho la razón por la que las organizaciones toman decisiones está dada más por la consecuencia negativa que el evento disruptivo trae per se, que la probabilidad de qué se evento ocurra y en ese orden de ideas, modelos matemáticos han determinado que en muchos casos la consecuencia es 1.5 veces la probabilidad lo que significaría, una torta del 40% de la probabilidad y un 60% de la consecuencia, así las cosas, el esfuerzo debería enfocarse en ese componente del 60% y desarrollar actividades de mitigación como sitios alternativos, planes de contingencia y/o diversificación del mercado y de la practica en la entrega de productos y servicios, entre otros, de esta manera reducir la consecuencia de ese evento disruptivo, indeseable o perturbador.

Una vez las organizaciones tienen definidos aquellos riesgos que son de mayor impacto para la organización, que tienen el potencial de interrumpir la continuidad de las operaciones y que ponen en riesgo la supervivencia y a la vez los intereses de sus partes interesadas, es necesario entonces establecer cuál es la probabilidad de qué dicho evento ocurra.

En la mayoría de los modelos se ha definido la probabilidad como primera tarea, y la consecuencia como segunda; sin embargo, los eventos que se referencian en la bibliografía dan cuenta de lo relevante que es para una organización atender en principio la consecuencia y de manera posterior la probabilidad, esta última, está determinada por algunos factores asociados a la susceptibilidad que tienen los activos y los procesos frente a la amenaza y su propia vulnerabilidad. Según un estudio realizado por Bologna y Wells, 20% de la población es deshonesta (centralizando acá el potencial de la amenaza) mientras que 20% es honesta especialmente por miedo a ser descubierta (¿qué pasaría, entonces, si supiera no va a ser descubierta? Y el 60% restante actúa dependiendo de las circunstancias; entonces, la probabilidad tiene un componente del 20% en la amenaza y en la vulnerabilidad el 80%.

Identificar cuáles son los procesos críticos y sus activos conlleva a revisar, entonces, a qué tipo de riesgos están expuestos, ya que la materialización de ese riesgo expone la continuidad de las operaciones, una vez identificado el riesgo es necesario determinar qué tan probable es que ese riesgo se pueda materializar, por un lado determinar cuál es la amenaza que tiene o que podría tener intenciones motivaciones pero sobre todo capacidades para afectar este tipo de activos, y del otro lado, la amenaza pudiera interpretarse no con un origen humano deliberado sino de origen accidental natural o ambiental. Adicional a lo anterior es necesario determinar qué tan vulnerable o qué tan susceptible son las operaciones y los activos críticos a partir de sus propias debilidades, con estos criterios, en principio es viable determinar cuál es el nivel de riesgo en este tipo de activos.

La criticidad y que en alguna literatura se encuentra como gravedad, severidad, impacto o consecuencia; está determinada por varios conceptos que se asocian inactividad del *core business*, como el Tiempo Máximo Tolerable de Indisponibilidad (MTPD por sus siglas en inglés) que es un espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas inaceptables, es decir el tiempo de inoperatividad hasta que logra su recuperación; otro concepto es el Tiempo De Recuperación Objetivo (RTO por sus siglas en inglés) y es el tiempo transcurrido entre la interrupción y la recuperación del servicio a un nivel aceptable, aún sin haber llegado al 100%; otro aspecto importante es el Punto De Recuperación Objetivo (RPO por sus siglas en inglés) y es el rango de tolerancia que la organización puede tener sobre una pérdida de datos producida por un evento relacionado con el desastre.

Aún así, a los conceptos de continuidad de operaciones se agregan conceptos de manejo de crisis como lo son las emergencias, los siniestros y los desastres; que pudieran, no solamente afectar la continuidad, sino también afectar las pérdidas humanas y perdidas reputacionales.

El Análisis del Impacto en el Negocio (BIA por sus siglas en inglés) ayudan a determinar; primero, cuáles son los procesos críticos que mantienen la supervivencia del negocio y segundo, a través de los conceptos de MTPD, RTO y RPO, determinar qué tan graves para la organización estos tiempos improductivos que pudiera llevar al cierre total de la organización, el mismo BIA, puede determinar cuando los costos de pérdida superan el valor de los activos; un ratio de rentabilidad de las organizaciones es el Retorno Sobre

los Activos, (ROA por sus siglas en inglés) calcula en qué medida los activos contribuyen a un beneficio basado en ingresos, cuando ese retorno es negativo, es decir es mayor la pérdida que el costo del activo, la organización empieza a comprometer su supervivencia, ese retorno basado en el flujo de caja operativo está por debajo de la expectativa de las partes interesadas incluyendo los socios de la organización.

El BIA entrega información sobre qué tanto puede perder una organización en un tiempo determinado y establecen la entrada para apalancar los proyectos o las iniciativas tanto en prevención como como en mitigación, de tal manera que la relación costo-beneficio va a determinar que la organización tiene la oportunidad de reducir la probabilidad y reducir el impacto en un porcentaje tal, que solamente compromete una decisión de implementar programas de seguridad costo efectivos.

Pasando de una máxima pérdida posible a una expectativa anual de pérdida

Los modelos exclusivamente preventivos, que trabajan sobre la reducción de la probabilidad son insuficientes, frente a la expectativas de las partes interesas, sobre todo porque atienden solo una parte del problema, y en particular la parte mas pequeña, esto significa que aunque se pueda establecer que tan probable es que un riesgo ocurra, se desconoce cuál es el impacto o la consecuencia de su materialización, así las cosas, sin su medición y sin su mitigación, lo que se asume es una máxima pérdida posible, inclusive por encima del valor de la propia empresa y sus activos, en el entendido que muchas operaciones de cadena de suministro mantienen en sus instalaciones, activos que no son de su propiedad, aunque una póliza de seguro pueda cubrir una pérdida, nunca será suficiente para resarcir un daño que afecta la reputación y la continuidad de la operación.

Esta pérdida máxima puede ir desde pérdida de vidas humanas, pérdidas de mercado, pérdidas operacionales, pérdidas ambientales, hasta pérdidas económicas. Sin embargo una manera de apalancar los proyectos de seguridad es precisamente, la oportunidad de comparar lo que se puede perder, versus, lo que vale reducir la oportunidad de que eso suceda más la limitación del impacto si llega a suceder; en esa alternativa es importante considerar por una lado que tan probable es que eso ocurra y cuánto vale minimizar su potencial de

ocurrencia, siendo esto último lo que afecta la continuidad de las operaciones; es decir va a ser necesario establecer cuánto vale reponer los equipo de la función critica, cuánto vale el alquiler mientras se reponen los equipos de la función critica, cuanto se asumen por el lucro cesante teniendo una operación detenida, con cuanto castiga el banco en ese interés al usar el dinero para una actividad de recuperación del desastre y en algunos casos cuanto pudiera recuperar por una indemnización vía seguro.

Una vez calculado los costos del estado de inoperatividad que superan los tiempos aceptables para la resiliencia organizacional, es posible determinar, no medidas técnicas exclusivamente, sino también administrativas y asumir esos riesgos residuales ya calculados, entendidos en este artículo como la pérdida esperada en el concepto de la Expectativa Anual de Pérdida.

Conclusión

Para enfrentar los recientes acontecimientos mundiales (conflictos armados, pandemias, ataques cibernéticos, manifestaciones populares violentas) se ha medido la capacidad de las organizaciones para lograr una preparación adecuada y administrar impensables situaciones que puedan poner en peligro el futuro de las mismas. Así, las organizaciones participan en un proceso global que describe genéricamente como Continuidad de Negocio, basados en criterios reales que permiten su gestión y sobre todo el patrocinio de las diferentes iniciativas. Las amenazas actuales requieren la creación de criterios objetivos enmarcados en un proceso permanente interactivo que sirve para asegurar la continuación de las actividades básicas de la organización antes, durante, y lo más importante, después de un evento de crisis.

En los términos más sencillos, es una práctica rentable para una empresa para proteger sus activos, no solo desde la reducción de la probabilidad, es necesario, ahora con mayor énfasis, la reducción del impacto y/o consecuencia. La alta dirección, en procura de los objetivos estratégicos debe estar preparada para presupuestar y obtener los recursos necesarios y hacer que esto suceda. Por lo cual, las organizaciones deben disponer de una infraestructura administrativa adecuada para afrontar con eficacia la gestión de crisis. Esto asegurará que todos los interesados entiendan cómo se toman las decisiones implementadas, y cuáles son las funciones y responsabilidades de los participantes.

La velocidad que impone la globalización y la actual dinámica de los negocios, donde los aspectos de oportunidad y disponibilidad cobra mayor relevancia, hace que la interrupción del servicio en la organización, pueda tener un impacto que ponga en peligro no solo la buena marcha del negocio sino su misma supervivencia. El abanico de amenazas es cada vez mayor y por consiguiente los riesgos aumentan, mostrando la necesidad de crear estrategias que puedan mantener la continuidad de las operaciones en diferentes escenarios y dirigidas a los riesgos a los que se está expuesto. Así las cosas, las organizaciones se comprometen a llevar a cabo todas las medidas razonables y apropiadas para proteger a las personas, los bienes y los intereses empresariales, frente a eventos indeseables y perturbadores que tengan el potencial de afectar la continuidad de las operaciones. Razonables y apropiadas se refiere al resultado del uso apropiado criterios para gestionar la continuidad del negocio en operaciones de cadena de suministro.

Referencias

- Handbook Fraud and Commercial Crime Prevention, Handbook Fraud and Commercial Crime Prevention
- Protocolo de acompañamiento a la reactivación de la producción, ONUDI, Mincomercio
- Resiliencia organizacional y sistemas de gestión de la seguridad para la preparación y continuidad requisitos con orientación para su uso, ASIS internacional
- A Guide to Business Continuity Planning, James C Barnes
- Business Continuity Management Systems: Requirements with Guidance for Use ASIS International
- Business Continuity Management, how to protect your company, Michael Gallagher
- Business Continuity A Practical Approach for Emergency Preparedness Crisis Management a Disaster Recovery, ASIS International
- Contingency Planning and Disaster Recovery A Small Business Guide, Donna R. Childs
- Corporate crisis and Risk management: Modelling, strategies and application, M. Aba-Bulgu
- Dictionary of Business Continuity Management Terms, Lyndon Bird FBCI
- Disaster Recovery 100 Success Secrets, Gerard Blokdijk
- 101 World Class Expert Facts, Hints, Tips and Advice on Disaster Recovery, Dale Scott

- Organizational Resilience, Security, Preparedness and continuity Management Systems
- Practical Guide to Business Continuity Assurance, Andrew McCrackan
- Practitioner's Guide to Business Impact Analysis, Dan Swanson
- Risk Issues and Crisis, Management, Michael Regester
- Societal Security and Crisis Management, Lise H. Rykkja
- The Handbook of Risk Management Implementing a Post-Crisis Corporate Culture, Philippe Carrel
- The Project Surgeon A Troubleshooter's Guide to Business Crisis Management, Boris Hornjak
- The Changing Face of Strategic Crisis Management Risk, Crisis and Security Management Edward P. Borodzicz
- Business Risk Management Models and Analysis, Edward J. Anderson
- Metrics and Methods for Security Risk Management, Carl S. Young
- Fundamentals of Risk Analysis and Risk Management, Vlasta Molak
- The Handbook of Risk Management Implementing a Post-Crisis Corporate Culture, Philippe Carrel
- ISO31050 Guidance for managing emerging risks to enhance resilience, ISO International
- Sistemas de gestión de la continuidad del negocio: requisitos con orientación para su uso, ASIS International
- Quantitative Risk Management: Concepts, Techniques and Tools is a part of the Princeton Series in Finance, Darrell Duffie Stephen Schaefer
- Probability And Impact Rating System, Australian Prudential Regulation Authority
- General Security Risk Assessment , ASIS International
- Security Risk Management Body of Knowledge, Talbot Julian
- Quantitative Risk Assessment The Scientific Platform, Terje Aven
- Guide To Risk And Uncertainty Analysis Technical Guide Of The Assessment Framework The Assessment Framework, Infrastructure Australia 2021
- Doctorando PhD en Pensamiento Complejo Multiversidad Edgar Morín, México
- Mágister en Seguridad y Defensa Nacional de Escuela Superior de Guerra
- Maestrante en Compliance y Gestión de Riesgos, ADEN University
- Especialista en Administración de Seguridad de Universidad Militar Nueva Granada
- Arquitectura, Universidad Piloto de Colombia
- Profesional en Ciencias Militares, Escuela Militar de Cadetes Gral. José María Córdoba
- Consultor en Seguridad - Superintendencia de Vigilancia y Seguridad
- Certificado CPP - PSP, ASIS International
- Certificado Introductorio en Prevención del crimen a través del diseño ambiental CPTED por ICA

- Psico fisiólogo forense- Poligrafísta Profesional,
- Auditor Internacional de sistemas de gestión de control y seguridad BASC
- Auditor Líder ISO 28000 Seguridad en la Cadena de Suministro
- Auditor Líder ISO 37001 Antisoborno
- Instructor y Experto Técnico en Operaciones de Seguridad Norma ISO 18788
- Conferencista internacional, Docente en Maestrías, Especializaciones, Diplomados
- Ganador del premio "Regional Certification Award" de ASIS International 2010.
- Director de Consultoría en Riesgos con Mas de 20 años de experiencia en Prevención del Crimen Organizado Transnacional; Prevención de Lavado de Activos, Fraude, Soborno y Corrupción; Manejo de Crisis, Continuidad de Negocio y Resiliencia Organizacional.

CAPÍTULO 9

LAS CAPACIDADES INSTITUCIONALES EN SEGURIDAD DIGITAL AL SERVICIO DE LOS COLOMBIANOS

Por: Centro Cibernético PONAL/DIJIN

El cibercrimen es un fenómeno que por su naturaleza y génesis se ha caracterizado por ser multijurisdiccional y transfronterizo, por lo que las víctimas, delincuentes y escenas del crimen se pueden encontrar en diferentes latitudes del orbe.

A su vez, desde la academia se ha generado el debate con relación a la diferenciación de estos comportamientos que se ejecutan como medio o como fin, de tal forma que algunos de ellos en otrora se ejecutaban en un entorno físico, y con la irrupción de las nuevas tecnologías han mutado y diversificado su accionar a un entorno digital, como es el caso de las estafas, amenazas, calumnias, etc; pero a contrario sensu, han surgido nuevas amenazas en el ciberespacio que por su gravedad comprometen bienes jurídicos tutelados como es la información y los datos de los ciudadanos, y en consecuencia ha dado vida jurídica a nuevos tipos penales especializados, como es el uso del software malicioso, la denegación de servicios, el acceso abusivo a sistemas informáticos, entre otros.

Ante este escenario de retos que deben afrontar los Estados, y del cual Colombia no es la excepción, desde el año 2011 el país viene desarrollando una política pública, dirigiendo sus esfuerzos para fortalecer las capacidades institucionales y definir roles de interacción entre las entidades responsables que permitan avanzar en una respuesta oportuna y efectiva a las necesidades en seguridad digital bajo un modelo de gestión de riesgos que demandan nuestros ciudadanos.

Entre otras instancias que hacen parte de este ecosistema digital, realizan un papel protagónico las Agencias de Ley y su articulación internacional para adelantar investigaciones criminales transnacionales desde un ámbito multilateral, considerado hoy por hoy como un campo obligatorio, permitiendo desplegar acciones operacionales simultáneas, para la desarticulación conjunta de estructuras criminales dedicadas a este flagelo social.

Es por ello, que la Policía Nacional de Colombia a través del Centro Cibernético Policial de la Dirección de Investigación Criminal e INTERPOL, ha desplegado cuatro procesos que se integran bajo una sinergía armónica, como son la cooperación internacional policial y alianzas estratégicas, prevención, ciberinvestigación e informática forense, focalizadas a reducir las ventajas que el cibercrimen logra con el desarrollo de las nuevas tecnologías que garantizan

la intimidad y el anonimato, derechos que no discriman a ciudadanos de bien y ciberdelincuentes.

Es así como a través es la cooperación policial y sus instrumentos internacionales, donde la institución ha fortalecido la interacción con autoridades de otros países y agencias internacionales como EUROPOL (específicamente en el Centro Europeo del Cibercrimen - EC3), INTERPOL y Ameripol, FBI entre otros, para el intercambio de información estratégica y operacional, que permita la comprensión del estado del arte del cibercrimen y la construcción de inicitiavas investigativas transfronterizas.

A su vez, el sector privado es un actor fundamental para la institución, si aceptamos que gran parte de la información es administrada por multinacionales y empresas que prestan bienes y servicios, de allí que las alianzas estratégicas que se han consolidado con compañias para nombrar algunas como Facebook, Twitter e Instagram pero también con el sector financiero como lo son Asobancaria, Incocrédito y demás entidades bancarias, estas últimas donde se concentra buena parte de las intenciones criminales de estas organizaciones criminales, conllevan a un modelo de corresponsabilidad para garantizar mejores condiciones de ciberseguridad a los conciudadanos.

Por otra parte, el proceso de prevención que se enfoca en lograr un nivel de conocimiento y conciencia en los usuarios de Internet que permita comprender los riesgos inherentes del uso de las nuevas tecnologías, generando un escenario de acercamiento del ciudadano con nuestra institución a través de un servicio novedoso mediante la plataforma especializada CAI Virtual (http://caivirtual.policia.gov.co), además de ofrecer información del modus operandi y recomendaciones para no ser víctima de delitos informáticos, también permite interactuar a través de un chat 24/7 con un experto en ciberseguridad que gestiona incidentes cibernéticos, desde la pérdida de control de una cuenta de la red social hasta la verificación de correos electrónicos con archivos adjuntos que podrían contener software malicioso.

El tercer proceso que corresponde a la ciberinvestigación, está enfocado a la identificación y desarticulación de organizaciones conformados por actores criminales especializados que diversifican su accionar con vectores de ataque entre otros, con métodos sofisticados de ingeniería social, suplantación de sitios web para capturar datos personales, uso de software malicioso con capacidades

de infectar el sistema informático y escalar niveles de privilegio que conllevan a la obtención de datos personales y sensibles, y que comprometen gravemente a usuarios y compañías.

En consencuencia, este proceso mediante la Unidad Investigativa de delitos informáticos, bajo la Estrategia Integral de Ciberseguridad –ESCIB y la coordinación con la Fiscalía General de la Nación, ha logrado la judicialización en los últimos 3 años de más de 725 actores criminales, que han afectado el patrimonio económico de alcaldías, programas de restitución de tierras, pensiones, y diferentes cuentas bancarias de personas naturales y jurídicas, así como de aspirantes a créditos que fueron engañados por supuestas cooperativas; lo anterior sin dejar atrás, la afectación de rentas criminales de personas que atentan contra la integridad y el desarrollo sexual de los niños, niñas y adolescentes en Internet a nivel nacional e internacional.

Conviene subrayar, que esto no sería posible sin la obtención de la evidencia digital y el trabajo de laboratorios de informática forense, coadyuvando a la realización de estas investigaciones sólidas, a través del aporte técnico-científico respecto del acervo probatorio obtenido mediante técnicas especializadas de criminalística, siendo auxiliares de la administración de justicia bajo protocolos estandarizados, para la toma de decisiones de la Fiscalía General de la Nación.

Finalmente, es desde una óptica holística de prevención, disuasión, investigación criminal, políticas públicas y regulación homogénea de manera global, escenario en el que converge la participación activa desde las instituciones gubernamentales e internacionales como también el sector privado y la academia, entre otros, para disponer de capacidades proporcionales a los retos que antepone este fenómeno criminal.

CAPÍTULO 10

LA BUENA DEBIDA DILIGENCIA

Por: Mariano Sánchez CEO - Socio fundador Risk Internacional

El término **Debida Diligencia** o diligencia **debida** (en inglés: ***due diligence***) se emplea para la prevención de riesgos y en algunos casos para conceptos que impliquen la validación de una empresa o persona previa a la firma de un contrato. Puede tratarse de una obligación legal, pero el término comúnmente es más aplicable a investigaciones voluntarias. Un ejemplo habitual de diligencia debida en varias industrias es el proceso por el cual un comprador potencial evalúa una empresa objetivo o sus activos de cara a una adquisición.

La teoría de la debida diligencia sostiene que llevar a cabo este tipo de validación, contribuye significativamente a una toma de decisiones informada ya que optimiza la calidad y cantidad de información disponible de quienes toman estas decisiones y además asegura que esta información sea usada sistemáticamente para deliberar de una manera reflexiva la decisión en cuestión y todos sus costos, riesgos y beneficios.

- El término «due diligence» DEBIDA DILIGENCIA
- Conocimiento de la Contraparte
- KYC (Know Your Customer) Conozca a su Cliente

Se emplea para conceptos que impliquen la **"investigación"** de una empresa o persona previa a la firma de un contrato o una ley con cierta diligencia de cuidado. Puede tratarse de una obligación legal, pero el término comúnmente es más aplicable a investigaciones voluntarias.

> *"La Debida Diligencia consiste en la búsqueda y análisis de aspectos, positivos y negativos de una empresa o persona, que facilitan la toma de decisiones, cuyo desconocimiento de esos aspectos en algunos casos pueden llegar a poner en riesgo la existencia o continuidad de una inversión, transacción o negocio de cualquier naturaleza." Mariano Sánchez.*

La Debida Diligencia hace referencia a una validación establecida en la gestión interna del riesgo de la organización, donde se busca el aseguramiento en las relaciones contractuales con sus contrapartes en materia de prevención de los riesgos asociados al lavado de activos, financiación del terrorismo y la

proliferación de armas de destrucción masiva; donde las compañías están expuestas a los riesgos reputacionales, legales, operacionales y de contagio que podrían afectar ostensiblemente cualquier organización.

Las recomendaciones del Grupo de Acción Financiera Internacional (GAFI), en materia de conocimiento del cliente, establecen las recomendaciones: 10, 22, entre otras. En ellas hacen énfasis en la importancia de su aplicabilidad en diferentes sectores, su segmentación y continuidad en diferentes procesos que deben arrojar un análisis más intensificado que entregue información de una persona natural o jurídica; esta última que incluya su composición accionaria y societaria logrando llegar a los beneficiarios finales.

Citando el glosario de la **UIAF** es preciso traer al tema la definición que se tiene sobre la Debida Diligencia a Clientes:

> *"Las entidades deben tener un conocimiento efectivo, eficiente y oportuno de todos los clientes actuales y potenciales, así como para verificar la información y los soportes de la misma, es decir de todas personas naturales o jurídicas con la cual la entidad establece y mantiene una relación contractual o legal para el suministro de cualquier producto propio de su actividad"*

En las circulares emitidas por las diferentes Superintendencias, se estipula la obligatoriedad de la gestión del *'Due Dilligence'* o **debida diligencia,** capacitaciones a los funcionarios en prevención, control y administración del riesgo de lavado de activos y financiación del terrorismo, y el envío de Reportes de Operaciones Sospechosas (ROS) a la **Unidad de Información y Análisis Financiero (UIAF),** entre otros.

La Debida Diligencia, verificación en listas vinculantes, restrictivas y no restrictivas, es una acción fundamental al interior de todos los sistemas de gestión del riesgo de lavado de activos y financiación del terrorismo, ahora también en los PTEE y en procesos de BASC y OEA.

Uno de los principales riesgos a los cuales puede verse expuesta una compañía es iniciar o mantener vínculos con personas incluidas en las listas de restrictivas o vinculantes. Las consecuencias desde los puntos de vista reputacional, legal, operativo y de contagio pueden llegar a afectar la continuidad de un negocio de la empresa, al punto de quedar envuelta en investigaciones, sanciones e incluso la muerte comercial.

Para suplir esta necesidad de información, existen una serie de herramientas que automatizan las consultas, validan y cruzan de manera amplia los distintos sistemas con información de personas y empresas, **listas restrictivas ALA/CFT** y que mitiga correctamente esta contingencia: la verificación en **listas de *Compliance*.**

Este procedimiento actual que usan las empresas que únicamente observan información negativa en repositorios estáticos de datos de las personas desconocen lo que realmente es la debida diligencia y en muchos casos ponen en riesgo las decisiones objetivas de los analistas.

La información completamente actualizada, en repositorios dinámicos, con información positiva de la persona, es mucho más relevante a la hora de gestionar riesgos y en debida diligencia.

Una buena debida diligencia consiste en primero conocer quién es la contraparte, saber su identidad o identificarla, cruzar sus datos; ya sea de persona natural o jurídica, saber si esta persona está viva o vigente, su nombre, cruzarla en línea con listas restrictivas, listas de sanciones y bases de datos de registros públicos de autoridades judiciales, Procuraduría, Contraloría y Policía con el fin de hallar alguna coincidencia de restricciones, sanciones, registros positivos.

La actualización de la información depende de la misma fuente de información y no del proveedor de listas y esto, es fundamental para garantizar que exista objetividad, actualización, eficiencia, pero lo más importante confianza.

Recordemos que la Debida Diligencia y este cruce de listas, en las que se incluyen las **Listas PEP** por ejemplo, se encuentra presente en varias de las etapas y elementos de un sistema de gestión del riesgo de lavado de activos y financiación del terrorismo.

A pesar de ser un instrumento efectivo, eficiente y necesario en los **SIPLAFT, SARLAFT, SAGRILAFT** y sistemas semejantes, en Colombia no existe un marco jurídico que defina detalladamente cuáles listados y bases de datos deben ser consultados; sin embargo, sí es cierto que mientras más completa y mayores fuentes de información sean consultadas, menor será el riesgo expuesto y mejores decisiones se tomarán.

La Debida Diligencia como proceso

La Debida Diligencia muchas veces se confunde con la validación de antecedentes, o *background check,* por su nombre en inglés, el cual es un conjunto de consultas sobre una persona o empresa para verificar su identidad, confirmar que es quien dicen ser y de esta manera evitar cualquier tipo de fraude, corrupción o lavado de activos.

Todos tenemos una historia y un perfil que responde a quiénes somos. Gran parte de esta información es pública y está disponible para la consulta, es de interés para quienes hacen una buena gestión de riesgos. Por ejemplo, las organizaciones del Estado y compañías del sector privado, en su mayoría revisan nuestro pasado antes de vincularnos a sus operaciones. Este proceso se conoce como **Debida Diligencia**.

Estas validaciones son muy frecuentes en los procesos de selección de personal o proveedores y constituyen una oportunidad para conocer los antecedentes o los históricos judiciales y penales de las personas. También permite conocer información acerca de empleos anteriores y la veracidad de los títulos, profesiones, documentos, soportes de la educación que la persona dice haber realizado.

Características de unas buenas fuentes de información de Debida Diligencia

1. Fuentes de información pública y de datos abiertos. Sin exposición de riesgo de incumplimiento de normas de hábeas data. Recordemos que recopilar datos personales sin la autorización del titular acarrea incumplimientos a las normas de Habeas Data, salvo algunas excepciones y fines.

2. Fuentes confiables, la ventaja de ir a los registros públicos de las autoridades es que la calificación de la confiabilidad de la información es alta.

3. Fuentes con información de Calidad de sus expedientes públicos oficiales. Lo cual genera objetividad a la hora de una noticia *"Fake"*.

4. Fuentes con registro oficial y público de todos los casos o asuntos; se encuentran todos los asuntos, los que salen en noticias y los que no.

5. Fuentes con registro de la identidad de los implicados, evita la homonimia, situación que amplía el índice de margen de error en una debida diligencia.

6. Fuentes Requeridas como buenas prácticas de Debida Diligencia exigidas por las diferentes Superintendencias, por ejemplo, la Superintendencia de Sociedades, sugiere que dentro de la debida diligencia a las contrapartes se consulte la página de Antecedentes de Policía Nacional, Antecedentes de Procuraduría, Antecedentes fiscales de la Contraloría entre otras.

Las operaciones inusuales, las sospechosas y la debida Diligencia

Para minimizar las actividades riesgosas o sospechosas, las empresas deben conocer adecuadamente a sus contrapartes, identificar jurisdicciones vulnerables, todo lo cual les evitará ser asociadas con actividades LA/FT.

Recordemos, que las operaciones inusuales son aquellas operaciones irregulares o extrañas, cuya cuantía o características no guardan relación con la actividad económica de las contrapartes o que, por su número, cantidades transadas o particularidades, se salen de los parámetros de normalidad establecidos para un rango de mercado de un grupo de usuarios determinados. Las operaciones sospechosas, además de la inusualidad, se caracterizan porque la operación no puede ser razonablemente justificada.

Se consideran, en especial operaciones sospechosas, aquellas operaciones complejas, importantes, significativas, que no respondan a los patrones de transacciones habituales, que carecen de fundamento económico o legal razonable; que por su naturaleza o volumen no correspondan a las operaciones activas o pasivas de las contrapartes según su actividad o antecedente operativo y que no tienen una causa que las justifique.

Existen diferentes métodos para calificar y detectar operaciones sospechosas. A través de la inteligencia proactiva, se analiza la información que permite identificar áreas vulnerables o problemas para predecir comportamientos o para detectar situaciones riesgosas.

La inteligencia proactiva en materia de cumplimiento y de gestión de estos riesgos, integra la tecnología, las herramientas analíticas, el conocimiento del

negocio y los canales de comunicación con el fin de generar un monitoreo periódico o permanente, acciones de mitigación, notificaciones y alertas de seguridad.

En todas las organizaciones, el Oficial de Cumplimiento debe conocer las actividades de sus contrapartes, la magnitud de sus operaciones, solicitar información financiera, contable actualizada, así como soportar las características básicas de las transacciones.

La debida diligencia y la validación de antecedentes

La debida diligencia incluye las acciones necesarias para conocer adecuadamente a las contrapartes, reforzando el conocimiento de aquellos que por su actividad o condición sean sensibles a riesgos LA/FT. De esta manera se cumplen con las obligaciones establecidas en la normatividad aplicable, el Manual de Políticas, el Código de Conducta y en las disposiciones aplicables para prevenir actividades LA/FT de la manera más eficiente y diligente posible.

La debida diligencia es el cuidado razonable de las empresas para prevenir la exposición al riesgo de actividades (LA/FT). La piedra angular de todo buen Sistema de Prevención de Riesgos de Lavado de Activos y Financiación del Terrorismo (LA/FT) es la adopción e implementación de directrices y procedimientos de debida diligencia.

Las Debidas Diligencias en línea

En Compliance.com.co prestamos este servicio en línea para facilitar y hacer más rápida la consulta de múltiples bases de datos y descarga de resultados.

Nos interesa mucho que se analice mejor la información y no nos preocupemos por buscarla. Se cree que un analista de riesgo o la persona que dedica su tiempo a validar personas y empresas, emplea más tiempo buscando la información que en analizarla. La idea es hacerlo al revés para obtener mejores resultados de análisis.

Creemos que nuestro servicio es el más eficiente del mercado, sabemos que es necesario ir un paso adelante y por eso contamos con el mayor alcance esperado,

pues los resultados se obtienen de forma inmediata y a un solo clic en menos de un minuto, como si fuera una Debida Diligencia Ampliada. Contamos con operaciones en varios países de Latinoamérica, incluyendo Colombia, Perú y México.

Nuestra plataforma de validación en línea, permite hacer consultas masivas o en *batch* de hasta 15.000 personas o empresas a la vez en más de 1.400 fuentes de información pública y en más de 1.670 bases de datos públicas, nacionales e internacionales.

También si así lo desea el cliente, gestionar sus alertas y mantener monitoreadas sus contrapartes ante un eventual cambio del estado del riesgo. Situación relevante para tomar decisiones con oportunidad y salir siempre un paso adelante a la delincuencia común y organizada.

Consideramos que los procesos de debida diligencia, de validación de antecedentes o *background check* como medida preventiva brindan tranquilidad y generan confianza. Aseguran de que las personas con las que interactuamos son quienes dicen ser.

Prevenimos así, que el Lavado de activos, el Fraude, la Corrupción y otros delitos toquen las puertas de nuestras organizaciones. Depende de usted. Tome decisiones seguras.

Conozca más acerca de nosotros entrando a nuestra página web www.compliance.com.co, solicite más información al correo electrónico contactos@compliance.com.co.

Fuentes:

- Módulo general Curso: *Lo que debe saber sobre lavado de activos y la financiación del terrorismo UIAF*
- Circular 100-000006 – agosto 2016 Superintendencia de Sociedades
- Libro Modelo de Administración de riesgos de lavado de Activos y financiación del terrorismo (LA/FT). Oficina de las naciones unidas contra la droga y el delito UNODC y cámara de comercio de Bogotá.

CAPÍTULO 11

HACIA UNA ESTRATEGIA INTEGRAL PARA BLINDAR A LAS EMPRESAS DE LAS ECONOMÍAS CRIMINALES

Por: BG® Juan Carlos Buitrago Arias
Policía Nacional de Colombia
Founder & CEO StrategosBIP

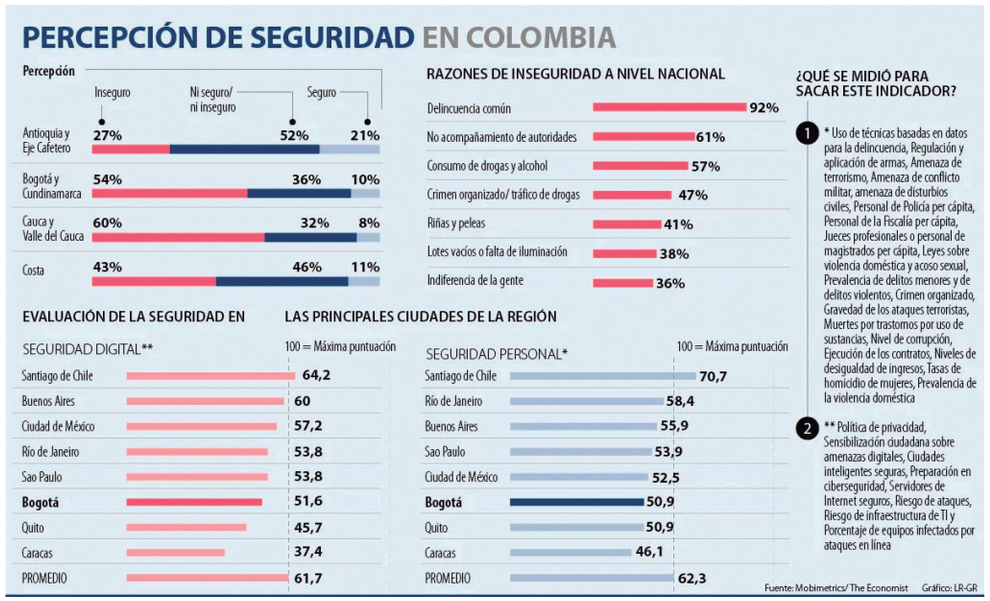
A pesar de la disminución en los índices de delitos de alto impacto en el país, como lo son el hurto[1] y el homicidio[2], la percepción ciudadana frente a la inseguridad está disparada, es generalizada y perdura en el tiempo sin importar que los índices mejoren. Lo anterior se sustenta con la encuesta de *Mobimetrics*, que, para 2021, señala que el 45% de las personas encuestadas percibe sus ciudades como inseguras. Esta estadística se retroalimenta con la encuesta de Pulso Social realizada por el Departamento Administrativo Nacional de Estadística (DANE) en 2022, donde *"el 57,1% de los hombres y el 50,3% de las mujeres tienen alta percepción de inseguridad, mientras que, en 2021, las cifras eran del 53,5% para los hombres y 50,6% para las mujeres"* (Portafolio, 2022).

Los flagelos criminales siguen impactando negativamente la percepción no solo de los individuos sino también de los gremios empresariales, quienes de acuerdo con la Encuesta de Clima de Negocios (2021), liderada por la Cámara de Comercio de Bogotá (CCB), el 87% de los empresarios perciben a Bogotá como insegura, porcentaje que aumentó en un 37% comparado con la medición de 2020.

[1] De acuerdo con datos de la Policía Nacional, citados por Joel Escobar de Radio Nacional de Colombia, en el primer semestre del año se ha presentado una reducción del 13% en las denuncias de hurtos en el país para los primeros cinco meses del 2022, en comparación al mismo periodo del año anterior. Según la Institución, en lo corrido de este año, se han presentado más de 123 mil casos de robos, mientras que en el 2021 fueron 140 mil para el mismo periodo, entre enero y junio.

[2] Según el Centro de Análisis de Datos *Delfos*, de la Universidad Externado de Colombia, *"en el primer semestre del 2022 bajaron notoriamente los homicidios comparados con el primer semestre de 2021. En 2021 hubo cerca de 6800 muertes violentas versus las 6611 de 2022. Esto se traduce en una disminución entre el 2% y 3%."*

Gráfico 1: Encuesta Mobimetrics sobre percepción de inseguridad en Colombia (2021).



Fuente: Acosta, (2021), en: https://www.asuntoslegales.com.co/actualidad/los-indicadores-que-rajan-a-colombia-en-temas-de-seguridad-individual-y-cibernetica-3224028

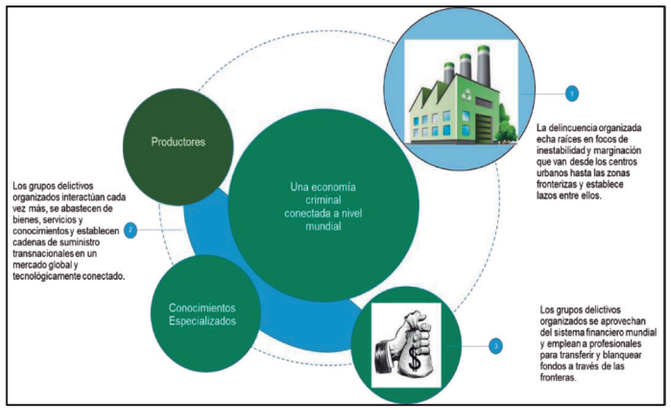
Ante este crítico panorama, los expertos han analizado las causas de esta situación para proponer nuevas estrategias que inciden categóricamente en la disminución de los índices de aquellos delitos de alto impacto, tanto para los individuos como para las empresas, pero que también abonen positivamente a la percepción de seguridad.

Los analistas convergen en argumentar que los fenómenos criminales que afectan las condiciones de seguridad de los ciudadanos y las corporaciones, son perpetrados por estructuras organizadas que trascienden la delincuencia común, e incluso la absorben a través del "outsourcing criminal"; que dependiendo de sus capacidades y recursos despliegan sus actividades criminales a nivel zonal (barrios, localidades, ciudades), e incluso a nivel nacional y transnacional, con

discrecionalidad desmedida para aplicar violencia con diversidad de métodos. Estas estructuras organizadas actúan dentro de un engranaje sistémico ilícito, con claro enfoque lucrativo como motivación. Se observa en consecuencia, una evolución hacia una criminalidad corporativa, hacia el crimen como empresa, hacia un *Sistema de Economía Criminal*[3] entendido como, las dinámicas de construcción, consolidación y ampliación de rentas ilegales, desempeñadas por estructuras del crimen organizado claramente definidas, sean estas jerárquicas -en su mayoría- u horizontales, las cuales tiene una enorme capacidad adaptativa frente a cambios en su entorno y su organización misma.

El crimen organizado como género se compone de estructuras, organismos y/o sociedades que responden a estímulos externos, primordialmente el económico, cuentan con modelos operativos, estrategias a corto, mediano y largo plazo, incluso, alianzas estratégicas, con el propósito de obtener el máximo beneficio con el mínimo riesgo.

Gráfico 2: Esquema de la Economía Criminal.



Fuente: Elaboración propia con información de UNODC, (2022). Guía práctica para elaborar estrategias de alto impacto contra la delincuencia organizada, en: https://sherloc.unodc.org/cld/uploads/pdf/Strategies/Strategy_Toolkit_SP.pdf

[3] Villamil (2021), Sistemas Complejos de Economía Criminal.

Partiendo de la base que la principal motivación de las estructuras delincuenciales organizadas es la maximización del lucro, estas han prestado especial aten-ción en las empresas y corporaciones como objetivos predilectos de sus actividades delictivas, y como una de las más importantes fuentes de ingreso en sus procesos de diversificación de rentas ilegales-criminales. Es por tal razón, que el presente artículo, enfoca su atención en esta problemática y busca plantear estrategias de vanguardia que coadyuven a blindar a las empresas de la amenaza creciente que representan las economías criminales. Para ello, en primera instancia, se caracteriza de manera contextualizada el impacto de las economías criminales en la dinámica empresarial, luego se formularán desde el nivel estratégico algunas recomendaciones que le permitan a las corporaciones protegerse, controlar, responder y neutralizar el riesgo y finalmente se cierra con sendas reflexiones concluyentes al respecto.

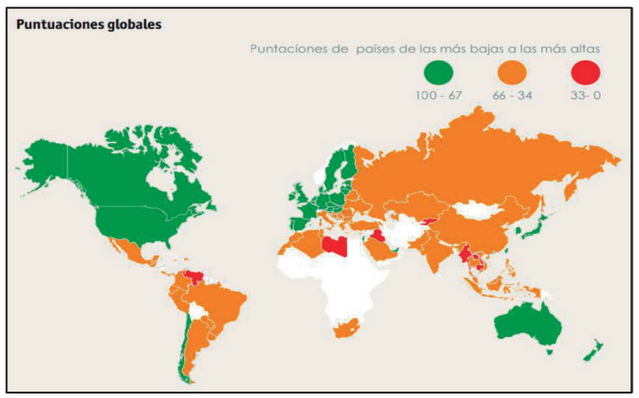
Impacto de las Economías Criminales sobre las empresas.

Las economías criminales afectan a las empresas desde diversos frentes: ciberataques, actos de corrupción, actividades de comercio ilícito, violaciones a la propiedad intelectual, extorsiones (vacunas), vinculación con el lavado de activos, por mencionar algunos de los riesgos criminales. Todas estas actividades generan a su vez ingresos económicos que perpetúan y sostienen la actividad criminal en el largo plazo; por ello se consideran sistémicas.

Según información de la UNODC, la OCDE, Cybersecurity Ventures & GFI, las ganancias de los principales delitos transnacionales son: falsificación y contrabando (US$464.000 millones); narcotráfico (US$320.000 millones); tráfico de armas (entre US$170-320.000 millones); trata de personas (US$150.000 millones); tráfico ilegal de petróleo (US$10.800 millones); cibercrimen (US$12.000 millones); y tráfico de vida salvaje (US$10.000 millones).

En el caso de la falsificación y el contrabando, estas modalidades del comercio ilícito representaron para 2019 aproximadamente el 2,5% del comercio mundial, según la OCDE. Cifras que se complementan con las aportadas por Carlos Loaiza, presidente de la Cámara de Comercio de Quito (CCQ), quien afirma que a nivel mundial el contrabando genera alrededor de USD 210. 000 millones anuales, representando para Latinoamérica entre el 1% y el 2% del PIB regional.

Gráfico 3: Índice del Entorno Global del Comercio Ilícito (2018)



Fuente: El Índice del Entorno Global del Comercio Ilícito, (2018), pp.9. Disponible en, http://illicittradeindex.eiu.com/documents/ECO043%20Illicit%20Trade%20WHITEPAPER%20ES%203.pdf

Gráfico 4: El Índice del Entorno del Comercio Ilícito en las Américas (2018)

AMÉRICAS		
CLASIFICACIÓN	PAÍS	PUNTUACIÓN/100
1	EE.UU.	82,5
2	Canadá	77,4
3	Chile	69,1
4	Argentina	64,0
5	Uruguay	63,0
6	Colombia	61,6
7	Cota Rica	60,6
8	México	58,6
9	Panamá	55,0
10	Perú	54,8
11	Brasil	50,6
12	Ecuador	50,1
13	Guatemala	46,0
14	Jamaica	43,7
15	Paraguay	43,3
16	República Dominicana	42,7
17	Trinidad y Tobago	38,0
18	Belice	34,7
19	Venezuela	28,1

Fuente: El Índice del Entorno Global del Comercio Ilícito, (2018), pp.9. Disponible en, http://illicittradeindex.eiu.com/documents/ECO043%20Illicit%20Trade%20WHITEPAPER%20ES%203.pdf

El comercio ilícito impacta directamente a las empresas del mundo, pues por medio de la competencia abiertamente desleal que supone la falsificación, la piratería, el contrabando, se desincentiva el comercio, el empleo formal, la creación de empresa y la innovación. Adicionalmente se afectan los ingresos tributarios y, peor aún, en algunos casos esto supone altos riesgos sanitarios para los consumidores, como es el caso de la falsificación de medicamentos.

De acuerdo con la OCDE en su informe de 2019, China, Hong Kong y los Emiratos Árabes son los mayores proveedores de mercancías falsificadas (piratas) y de contrabando. Colombia se encuentra entre los 25 países en donde más se elaboran productos falsificados (puesto 22). La Asociación Nacional de Industriales de Colombia (ANDI) agrega además que el contrabando y la falsificación tienen un impacto del 25% en el valor agregado y el 8% en la producción, para la **industria metalmecánica;** 11% en el valor agregado y el 8% en la producción, para la **industria de textiles y confecciones;** 5% en el valor agregado y el 3% en la producción, para la **industria de licores;** 29% en el valor agregado y el 14% en la producción, para la **industria de dispositivos médicos;** y 16% en el valor agregado y el 6% en la producción, para la **industria de alimentos.** Impidiendo que se generen más de 155.000 plazas de empleo y el 6.10% de incremento en la producción manufacturera.

La falsificación y el contrabando como fenómenos protuberantes en las tipologías del comercio ilícito, son actividades encubiertas, toleradas y normalizadas, gracias a los altos índices de corrupción estatal y bajos índices de cultura de legalidad e integridad moral, tanto en los funcionarios estatales como en los ciudadanos, y también en la empresa privada; no solo de Colombia[4] y Latinoamérica, sino del mundo entero, así se desprende del índice de percepción de la corrupción (2021), emitido por Transparencia Internacional.

[4] Que se ubica en el meridiano de la medición con 39/100 puntos.

Gráfico 5: Índice de Percepción de Corrupción (2021)

Fuente: Poder Ciudadano (2022). Índice de Percepción de Corrupción 2021 en, https://poderciudadano.org/indice-de-percepcion-de-corrupcion-2021-argentina-sigue-en-deuda/

Estrategias para blindar a las empresas y corporaciones de las Economías Criminales.

1. Metodología de Análisis.

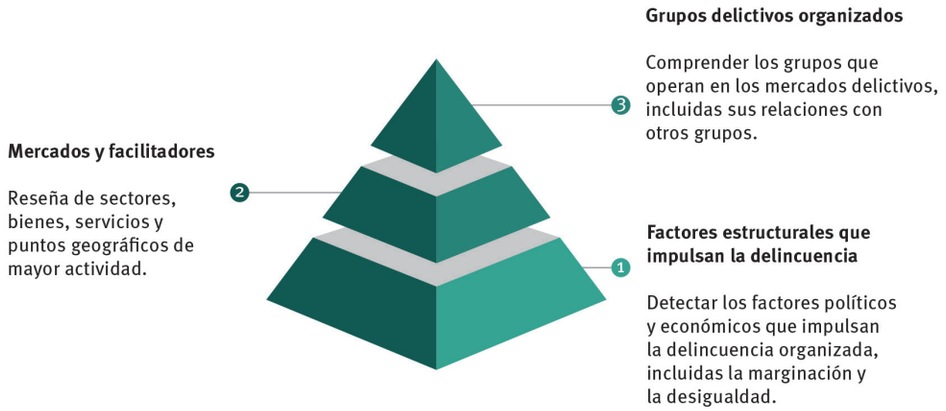
Antes de aventurarse a formular estrategias para proteger a empresas, individuos e incluso Estados, se debe adoptar una metodología que permita obtener los resultados deseados. Primero, sugerimos acudir a lo planteado por UNDOC (2022), cuando indica que es imperativo realizar un análisis estratégico de las economías criminales y por supuesto de quienes las desempeñan, es decir el crimen organizado. De acuerdo con el organismo anteriormente mencionado, el análisis estratégico debe abarcar al menos tres (3) dimensiones:

En primer lugar, es necesario comprender los factores estructurales y del entorno que promueven la delincuencia organizada y sus dinámicas de economía criminal; los cuales le permiten generar una estrecha vinculación, validación y aceptación por parte de la comunidad, volviendo el fenómeno criminal inherente a esta. Los factores a los que se hace referencia son entre otros, la inestabilidad y exclusión sociopolítica y económica, la desigualdad económica, la falta de cobertura de servicios públicos básicos y la corrupción. Esta visión contribuye a comprender las fuentes de legitimidad de las estructuras criminales y sus dinámicas, así como su rol e intereses, que, la mayoría de las veces disfrazados de reivindicaciones sociopolíticas, tiene un trasfondo lucrativo.

En segundo lugar, se deben analizar los Sistemas de Economía Criminal y donde se desempeñan. En esta dimensión se profundiza sobre los distintos lugares, bienes, servicios, facilitadores e infraestructuras que, en conjunto, componen las economías criminales. Entre los facilitadores en mención están: El sistema bancario y financiero, y todo mecanismo de transferencia de fondos; utilizado por las estructuras criminales para lavar su dinero y movilizar sus recursos. El sector inmobiliario, utilizado por las organizaciones delincuenciales para la adquisición de activos y la preservación de su valor en el tiempo, por supuesto, como instrumento para el blanqueo de capitales. Y finalmente, los medios de transporte -marítimo, terrestre y aéreo en sus distintas modalidades y variaciones-; como facilitadores para el transporte de mercancías y productos ilegales. Es fundamental que aquí se georreferencien los puntos críticos como las zonas fronterizas -puertos y trochas-, los centros urbano-rurales y los lugares de transbordo de personas y mercancías como puertos, aeropuertos y zonas francas.

En tercer lugar, es imperativo realizar el análisis sobre las organizaciones criminales (su estructura, jerarquía, miembros, ubicación y actividades). Así mismo, es importante indagar sobre sus enlaces nacionales e internacionales, para determinar sus capacidades y su rango de acción. La inteligencia e investigación criminal, por medio de mapas de relaciones con información de fuentes abiertas como redes sociales, pueden ser de utilidad para entender y conocer mejor los vínculos entre las distintas estructuras y sus facilitadores.

Gráfico 6: Dimensiones de un análisis estratégico.



Fuente: UNODC, (2022), pp. 10, en: https://sherloc.unodc.org/cld/uploads/pdf/Strategies/Strategy_Toolkit_SP.pdf

Aunado a las tres (3) dimensiones del análisis estratégico anteriormente mencionadas, se deben tener en cuenta algunos pilares o principios generales de donde surjan las estrategias que protejan a las empresas de las estructuras del crimen organizado y sus dinámicas de economía criminal. A pesar de que los países y regiones tienen características y particularidades únicas, la formulación de estrategias y respuestas para combatir las economías criminales en todo el mundo pueden surgir de los siguientes pilares propuestos por la UNODC en 2022:

Gráfico 7: Pilares, Principios Generales ´Las 4P´s´, para afrontar la delincuencia organizada y sus economías criminales.

Fuente: UNODC, (2022), pp. 14, en: https://sherloc.unodc.org/cld/uploads/pdf/Strategies/Strategy_Toolkit_SP.pdf

A pesar de que estos principios son universales, su implementación y recursos deberán adoptarse conforme a las características del problema y temática determinada. Para el caso específico de los impactos negativos de las economías criminales sobre las empresas, se plantean las siguientes estrategias.

1. PREVENIR: La (re)infiltración de las estructuras del crimen organizado en las comunidades, la economía y las instituciones políticas. Para evitar que, en un contexto permeado por la criminalidad, las empresas y corporaciones sean los objetivos predilectos de las economías criminales. Este pilar promueve la creación de resiliencia frente a la delincuencia organizada y sus dinámicas, con el objetivo de evitar su infiltración en los sectores más vulnerables de la sociedad.

Para **prevenir** el impacto de las economías criminales sobre las empresas es necesario afrontar sus factores estructurales con campañas de información en colaboración con la academia, la empresa privada, la sociedad civil y los medios de comunicación. Las comunicaciones estratégicas constituyen una herramienta muy útil y eficaz para generar conciencia y sensibilización en la opinión pública, la academia, el sector privado, las autoridades y los decisores gubernamentales, sobre el riesgo creciente e inminente de las economías criminales en cada una de las dimensiones, estructuras y dinámicas del individuo, la sociedad y la empresa pública y privada. De ahí el significado de realizar campañas de comunicación asertivas, en medios tradicionales (televisión, prensa y radio), pero también en medios digitales, adonde debe llegar el mensaje sobre los perjuicios que causan estas economías ilícitas.

Asimismo, se debe reforzar la integridad y transparencia de las instituciones gubernamentales a través de las recientes plataformas de colaboración de Interpol, Europol, Ameripol, Afripol y Asiapol, con diferentes sectores y partes interesadas (como las fuerzas del orden, el sector privado, la academia y la sociedad civil), para intercambiar mejores prácticas, compartir conocimientos y reforzar la red internacional de colaboración. La integridad y transparencia también forman parte de las estrategias que tienen que asegurar las empresas en materia de ética y cumplimiento de la ley *(compliance)*.

Es imperativo prevenir la actividad de economías criminales teniendo una regulación sólida y un régimen de aplicación de la ley que la acompañe en los distintos sectores vulnerables (sector financiero, comerciantes de alto valor, sectores de la propiedad, contadores, etc.).

Ofrecer alternativas a las comunidades para evitar su participación en las economías criminales con programas de formación, incluidas opciones de sustento económico con permanente acompañamiento de las autoridades, cuyo ejemplo más acertado son las zonas de comercio legal implementadas en Colombia; una iniciativa gratuita, de acompañamiento dirigido a micro, pequeñas y medianas empresas (MiPymes), enfocada en el emprendimiento, la formalización y la productividad, como herramientas de construcción de una sólida cultura de legalidad. Esta iniciativa busca formalizar el empresariado dedicado al comercio por medio de acciones de capacitación y asesoría de diferentes entidades del Estado como: el régimen simple de tributación, la facturación electrónica, el Código Nacional de Policía, la ruta del

emprendimiento, entre otros; en este programa, pueden participar personas naturales y jurídicas que desarrollen actividades empresariales-comerciales.

En su planeación y nacimiento (2019), esta iniciativa cobijó a 500 comerciantes de los denominados `San Andresitos`, y contó con el apoyo y la participación del Ministerio de Hacienda, Ministerio de Defensa, Ministerio del Trabajo, Ministerio de Comercio, Policía Nacional de Colombia, Dirección de Impuestos y Aduanas Nacionales DIAN, Policía Fiscal y Aduanera, Colpensiones, Dirección de Inspección y Vigilancia, Cámara de Comercio, Alcaldías municipales, SENA, Confecámaras, FENALCO, IMPULSA, ANDI (Policía Nacional de Colombia, 2019), entre otras instituciones.

2.PERSEGUIR: A las estructuras del crimen organizado y “asfixiarlas” al impactar sus engranados sistemas de economía criminal y en consecuencia sus ganancias ilícitas. Este pilar tiene por objetivo destruir la cadena de economía criminal, que como consecuencia tiene la desarticulación de la organización criminal pues, el beneficio económico es su razón de ser, y sin este, desaparecen.

Ahora bien, para **perseguir** las economías criminales que impactan negativamente a las empresas, es fundamental desarticular el negocio de las economías criminales enriqueciendo la formación, capacidad y perfeccionamiento técnico de los organismos e instituciones encargados de hacer cumplir la ley y de administrar justicia, en particular sobre: la realización de análisis de inteligencia e investigación criminal. La planificación y realización de investigaciones, incluido el uso de técnicas y capacidades sensibles adoptando las nuevas tecnologías de la información y las telecomunicaciones, además de la cooperación internacional interinstitucional en casos relacionados con la economía criminal, son claves para intervenir efectivamente los fenómenos criminales dinámicos, adaptativos y cambiantes en pleno siglo XXI.

Las empresas juegan un papel central en la interposición de denuncias – en calidad de víctimas – así como a través del intercambio de información y evidencias necesarias para favorecer la acción de la justicia. Mecanismos de denuncia anónima son y serán muy relevantes para facilitar la recolección de información por parte de las autoridades aún en contextos donde las empresas se sienten amenazadas por grupos criminales.

Como complemento de lo anterior, se debe impulsar la desarticulación de las organizaciones criminales desde su raíz, persiguiendo su aparato financiero, y para ello es primordial fortalecer las unidades de inteligencia financiera de los países, utilizando herramientas y técnicas de investigación financiera eficaces como, coordinadoras centrales de inteligencia económica (incluidos los reportes de operaciones sospechosas) para apoyar las investigaciones. En este punto la cooperación del sistema financiero privado es vital para desarrollar la estrategia.

> 3. PROTEGER: A las empresas, vulnerables frente a las economías criminales para que no sufran daños físicos ni patrimoniales. Este principio reconoce el impacto negativo que las dinámicas de la delincuencia organizada infringen a la economía de las corporaciones.

Para **proteger** a las empresas y corporaciones del flagelo que suponen las economías criminales, es necesario constituir y consolidar asociaciones empresariales fuertes para contrarrestarlas. Para suministrar apoyo mutuo entre corporaciones blanco de la delincuencia, es indispensable afianzar los frentes de seguridad empresarial, que contribuyan además con estrategias y acciones en bloque en temas legislativos, normativos y operativos hacia una mayor eficacia en la prevención e intervención de los Sistemas de Economía Criminal.

A nivel individual, las empresas deben incluir dentro de sus planes de gestión de riesgos los incidentes criminales; esto les permitirá mitigar el impacto o daño causado con mayor diligencia, así como para preparase mejor ante la potencial ocurrencia de algún evento criminal.

También es crucial que las autoridades policiales y fiscales dispongan de recursos suficientes y canales de atención adecuados para ejecutar operativos de protección inmediata. Esto es particularmente relevante en acciones criminales que puedan poner en peligro la vida o integridad de las personas, como lo son, las amenazas originadas por falta de pago de extorsiones.

> 4. PROMOVER: La cooperación e integración entre el sector público y el privado, en las zonas de frontera; en un enfoque que abarque a la sociedad en su conjunto, incluyendo, su motor más importante: **El tejido empresarial.** Este pilar, que se encuentra en la Convención contra la Delincuencia Organizada, destaca la importancia de las asociaciones a nivel local, nacional e internacional y entre los sectores gubernamentales, no gubernamental y el privado.

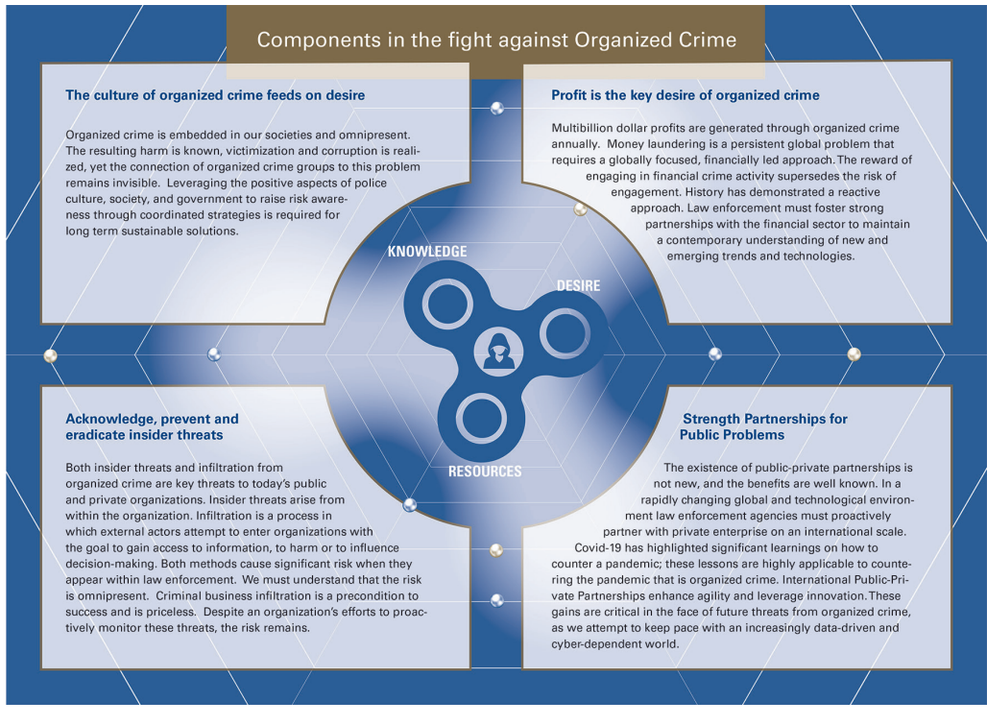
Finalmente, para **promover** la cooperación orientada a blindar las empresas de las economías criminales, se debe adoptar un enfoque multisectorial entre las partes interesadas (las autoridades estatales, los gremios empresariales, las MiPymes, las grandes empresas, las comunidades que se benefician de las actividades comerciales y empresariales en áreas específicas, etc.); en resumen, entre la sociedad civil, el gobierno y el sector privado, a nivel nacional e internacional.

Es fundamental, compartir la responsabilidad del problema, a través de una arquitectura de nivel institucional, que fortalezca la cooperación internacional y la asistencia judicial recíproca (por ejemplo, a través de las autoridades centrales y los órganos mixtos de investigación), así como reforzar los canales formales e informales de comunicación y diálogo.

Mejorar la cooperación en todos los niveles, al articular la cooperación policial, judicial y aduanera efectiva, mediante el establecimiento de convenios y mecanismos accionables que conduzcan a garantizar la eficiencia en la recolección de elementos materiales de prueba, el intercambio oportuno de información, la remisión de actuaciones penales, la extradición y el traslado de personas condenadas; son, en última instancia, herramientas disuasivas y punitivas para prevenir el impacto de las economías ilegales sobre corporaciones; protegerlas y perseguir a las estructuras criminales que a través de sus dinámicas económicas criminales las afectan.

Para culminar y como complemento de las propuestas anteriormente mencionadas, el Threat Agnostic Capability Ecosystem, elaborado por 30 policías del mundo en Barcelona, expone (4) componentes para luchar contra el crimen organizado y sus economías ilegales. Los cuatro componentes evidencian en el siguiente gráfico.

Gráfico 9: Componentes para luchar contra el crimen organizado y sus economías ilegales TRACE.



Fuente: TRACE (2022)

Referencias consultadas:

- UNODC, (2022). Guía práctica para elaborar estrategias de alto impacto contra la delincuencia organizada. Pp. 1-52. Recuperado el 7 de octubre de 2022 en, https://sherloc.unodc.org/cld/uploads/pdf/Strategies/Strategy_Toolkit_SP.pdf

- CCIT, TicTac & Safe. (2022). Tendencias del cibercrimen 2021-2022. Pp. 1-48. Recuperado en, https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

- Delfos - Centro de Análisis de Datos, (2022). Reducción de homicidios en el primer semestre de 2022 importante pero no suficiente. Universidad Externado de Colombia. Recuperado el 7 de octubre de 2022 en, https://www.uexternado.edu.co/delfos-centro-analisis-datos/reduccion-de-homicidios-en-el-primer-semestre-de-2022-importante-pero-no-suficiente/#:~:text=En%20el%20primer%20semestre%20del,violentas%20versus%206611%20en%202022.

- Portafolio, (2022). Aumentó la percepción de inseguridad en Colombia. Recuperado el 7 de octubre de 2022 en, https://www.portafolio.co/tendencias/aumento-la-percepcion-de-inseguridad-en-colombia-564748

- Poder Ciudadano (2022). Índice de Percepción de Corrupción 2021. Recuperado el 7 de octubre de 2022 en, https://poderciudadano.org/indice-de-percepcion-de-corrupcion-2021-argentina-sigue-en-deuda/

- Barona, G. (2022). Más de 80% de los empresarios percibe a Bogotá como insegura, según la CCB. Recuperado el 7 de octubre de 2022 en, https://www.larepublica.co/empresas/mas-de-80-de-los-empresarios-percibe-a-bogota-como-insegura-segun-la-ccb-3319664#:~:text=De%20acuerdo%20a%20la%20Encuesta,porcentuales%20en%20comparaci%C3%B3n%20con%202020.

- Escobar, J. (2022). En lo que va de 2022, los hurtos se redujeron un 13% en el país: Policía. Radio Nacional de Colombia. Recuperado el 7 de octubre de 2022 en, https://www.radionacional.co/actualidad/robos-en-el-pais-se-redujeron-13-en-lo-corrido-de-2022-policia

- ANDI. (s.f.). Mas País, cero contrabandos. Recuperado el 7 de octubre de 2022 en, https://www.andi.com.co/Home/Pagina/25

- Acosta, C. (2021). Los indicadores que rajan a Colombia en temas de seguridad individual y cibernética. Asuntos Legales. Recuperado el 7 de

octubre de 2022 en, https://www.asuntoslegales.com.co/actualidad/los-indicadores-que-rajan-a-colombia-en-temas-de-seguridad-individual-y-cibernetica-3224028

- Villamil, J. (2021). Sistemas Complejos de Economía Criminal, Análisis y focalización policial. Bogotá D.C.: Huella Forense.

- Ekos (2021) Contrabando, un mal que destruye la producción nacional y la competitividad de Ecuador. Recuperado el 6 de octubre de 2022 en, https://www.ekosnegocios.com/articulo/contrabando-un-mal-que-destruye-la-produccion-nacional-y-la-competitividad-de-ecuador

- OCDE. (2019). El comercio de productos falsificados representa ya un 3,3% del comercio mundial, y va a seguir aumentando, según la OCDE. Recuperado en, https://www.oecd.org/centrodemexico/medios/elcomerciodeproductosfalsificadosrepresenta.htm

- Policía Nacional de Colombia. (2019). Gran lanzamiento de las zonas de comercio legal: Un pacto por la legalidad. Recuperado en, https://oas.policia.gov.co/noticia/gran-lanzamiento-zonas-comercio-legal-pacto-legalidad

- Revista Semana (2019), Mal de muchos... Estos son los países más afectados por el contrabando. Recuperado el 7 de octubre de 2022 en: https://www.semana.com/edicion-impresa/la-grafica/articulo/cuales-son-los-paises-mas-afectados-por-el-contrabando/279963/

- El Nuevo Siglo. (2019). Ganancias de delitos trasnacionales: US$2,1 billones anuales. Recuperado el 7 de octubre de 2022 en: https://www.elnuevosiglo.com.co/articulos/05-2019-ganancias-de-delitos-trasnacionales-us21-billones-anuales

- Procuraduría General de la Nación, (2012). ESTUDIO SOBRE TENDENCIAS ECONÓMICAS DE LA DELINCUENCIA ORGANIZADA. Pp. 1-189. Recuperado el 7 de octubre de 2022 en, https://www.procuraduria.gov.co/portal/media/file/4%281%29.pdf

CAPÍTULO 12

LA GESTIÓN ANTIFRAUDE COMO UN PROCESO TRANSVERSAL

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

En los últimos años el mundo ha vivido un proceso de transformación digital acelerado que no se detiene y ha propiciado grandes cambios económicos, políticos y sociales.

En esta nueva era donde predomina el uso de la tecnología, las empresas han tenido que implementar el uso de este tipo de herramientas para responder a las exigencias del mercado, las cuales, así como han traído grandes beneficios, también se han convertido en un panorama muy atractivo para los delincuentes que se aprovechan de personas y empresas para obtener un beneficio mediante diferentes acciones.

La Asociación de Examinadores de Fraude Certificados (ACFE) en colaboración con Grant Thornton en una de sus más recientes publicaciones, "la próxima normalidad: prepararse para un panorama del fraude pospandemia" (2021), señalan que el 51% de las organizaciones han descubierto más fraudes desde el inicio de la pandemia, con una quinta parte indicando un aumento significativo en la cantidad de fraude detectado. Por su parte, solo el 14% de los encuestados reportan menos fraude durante este tiempo y el 71% espera que el nivel de fraude que impacta a sus organizaciones aumente.

En el informe de la Encuesta Global sobre Fraude y Delitos Económicos del año 2022 de PricewaterhouseCoopers (PwC) refiere que el 46 % de las empresas encuestadas experimentaron algún tipo de fraude u otro delito económico en los últimos 24 meses.

De igual forma, PricewaterhouseCoopers manifiesta que dentro de los riesgos más significativos para las empresas se encuentra el delito cibernético que se posicionó con un 36% como el de mayor ocurrencia y el más disruptivo, entre 19 eventos de fraude diferentes, seguido del fraude del cliente con un 26% y la apropiación indebida de activos con un 25%.

Adicional, los resultados de la encuesta muestran una amenaza creciente del fraude externo, ya que el 43% de las organizaciones reportan que este fue el incidente más significativo, seguido por el fraude interno con un 31% y en colusión entre fuentes externas e internas con un 26%. Esto quiere decir que casi en un 70% de los casos reportados existe participación de un agente externo en la comisión del delito

Por su parte, en el Informe a la Naciones del 2022 elaborado por la Asociación de Examinadores de Fraude Certificados (ACFE, por sus siglas en inglés), sobre

el fraude ocupacional, destaca que los estafadores a nivel interno siguen manteniendo sus esquemas y métodos a lo largo del tiempo. Dentro de estos se encuentran: la malversación de activos con 86% de los casos y una pérdida de USD$ 100.000 por caso, la corrupción con un 50% de los casos y una pérdida mediana de USD$150.000 y el fraude de estados financieros, que es la categoría menos común con un 9% pero con las pérdidas más significativa de hasta USD$ 593.000 USD por caso.

Respecto a la apropiación indebida de activos el Instituto de Gobernanza de Basilea en el Índice Antilavado (AML) de 2021, nuevamente indicó que el promedio de 110 jurisdicciones evaluadas aumentó el nivel de riesgo de 5.22 en 2020 a 5.30 en 2021.

Por otro lado, el Índice de Percepción de Corrupción (IPC) 2021, desarrollado por Transparencia Internacional, donde se analiza la percepción de corrupción en 180 países, con una escala entre 0 (corrupción elevada) y 100 (corrupción inexistente), señala que luego de la pandemia el nivel de corrupción se encuentra estancado en todo el mundo. El 68% de los países obtuvieron una puntuación inferior a 50 y el promedio global se sitúa en 43 puntos, igual que el índice del año 2020.

Según este índice, los países con mejor percepción son Noruega, Singapur, Suecia, Suiza, Países Bajos, Luxemburgo y Alemania, por lo que estás naciones se consideran las menos corruptas del mundo. Por su parte, dentro de los países que permanecen en las últimas clasificaciones se encuentran Sudán del Sur, Siria, Somalia, Venezuela, Yemen, Corea del Norte, Afganistán, Libia, Guinea Ecuatorial y Turkmenistán, en algunos de ellos, la corrupción se le atribuyen a los conflictos armados y regímenes autoritarios.

Respecto a las industrias más afectadas, casi dos tercios de las empresas de tecnología, medios y telecomunicaciones experimentaron algún tipo de fraude, seguido del sector de energía y servicios públicos, servicios financieros y la industria de la salud (PWC, 2022).

Así mismo, el reporte a las naciones de la ACFE 2022, sobre fraude ocupacional, refiere que las industrias más afectadas son: servicios bancarios y financieros con 351 casos y una pérdida media de US$100.000, gobierno y administración pública con 198 casos con pérdidas de US$150.000, fabricación o manufactura

con 194 casos y un costo de US$170.000 dolares, salud con 130 casos con un valor de US$100.000 y el sector asegurador que representó un total de 88 casos y una pérdida de US$130.000.

También KPMG en su estudio llamado “Una triple amenaza en las Américas” del año 2022, indica que el 83% de 600 directivos de múltiples industrias de la región, fue impactado por un ciberataque en los últimos 12 meses, el 71% experimento fraude interno o externo y el 55% sufrió pérdidas derivadas de multas regulatorias por incumplimiento.

Adicionalmente, el Informe global de Fraude e Identidad 2021, realizado por Data Crédito Experian, con datos de 2700 ejecutivos de negocios de América del Norte, América Latina, Europa, Medio Oriente y África, y Asia Pacífico, encontró que se incrementaron los reclamos relacionados con el fraude y el cibercrimen en Latinoamérica.

En Colombia, según lo mencionado por el Centro Cibernético Policial, en el 2020 se reportaron cerca de 35.184 incidentes informáticos, lo que evidencia un aumento del 82% con respecto al 2019 donde se presentaron un total de 19.298 casos. De los cuales el delito con mayor ocurrencia fue hurto por medios informáticos y semejantes con 13.212 casos, esto muestra un incremento del 34%, respecto al año anterior en donde se presentaron 9.861 casos. Adicional a esto, afirman que el delito que más creció fue suplantación de sitios web, pasando de 951 casos en 2019 a 4.353 casos en 2020, lo que refleja un crecimiento de este delito en un 358%.

La Cámara Colombiana de Informática y Telecomunicaciones (CCIT), el Tanque de Análisis y Creatividad de las TIC (TicTac) y su programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) reportan que solo en Colombia al finalizar noviembre de 2021, se presentaron 46.527 eventos por ciberdelitos en el país, registrando un crecimiento del 21% comparado con 2020.

Según el informe global sobre tendencias de fraude digital de TransUnion (2022) *“los casos de intentos de fraude digital crecieron un 52% a nivel mundial y un 134% en Colombia, al comparar 2019 con 2021, siendo el fraude relacionado al envío de mercancía el tipo de fraude que más aumentó”.*

Asimismo, el Índice antilavado de activos (AML) de Basilea 2021, refleja que, aunque Colombia pasó del puesto de calificación del 47 en 2020 al 32 en 2021,

el puntaje empeoró pasando de 4.62 en 2020 a 4.64 en el 2021, lo que refleja que aumentó el nivel de riesgo.

Adicionalmente, Transparencia Internacional en sus resultados del IPC 2021 refleja que Colombia obtuvo 39 puntos sobre 100 y se ubica en el puesto 87 entre 180 países evaluados, lo que revela que el país tiene niveles de corrupción muy serios, ya que su calificación se encuentra por debajo de 50 puntos.

¿Cuál es el impacto que tiene el fraude?

El fraude ocasiona consecuencias devastadoras, que impactan no solo a las empresas, sino a la población mundial en general. El impacto de la delincuencia económica se extiende a diferentes ámbitos y genera pérdidas monetarias, que en las grandes empresas representan el 1.5% del porcentaje de sus ganancias, 0.7% por fraude y 0.8% de las ganancias netas por multas por incumplimiento (KPMG, 20222). Estás pérdidas alcanzaron en el 18% de los casos los US$50 millones a nivel mundial (PWC, 2022).

En cuanto al fraude ocupacional, este generó pérdidas de más de US$ 3.6 mil millones durante el 2021.Con una pérdida promedio por caso de US$1,783,000. (ACFE 2022)

Por su parte, Según cifras del Cybersecurity Ventures sobre economía cibernética global, *en 2021 los costos por daños globales del cibercrimen ascendieron a los US$ 6 trillones, lo que equivale a US$ 648 millones en pérdidas por hora; US$11.4 millones un minuto y cerca de US$ 190.000 por segundo* (CCIT, TicTac y SAFE, 2021).

De igual forma, Luz Ángela Bahamón fiscal delegada contra las Finanzas Criminales en 2021 afirma que el lavado de activos en Colombia asciende en pérdidas a $6.2 billones, seis veces más que el año 2020, donde el valor fue de $800 mil millones (Infobae, 2021).

En cuanto a la corrupción, se estima en el mundo se pierden cerca de $US 400 billones anuales en corrupción en contratación pública (Transparencia Internacional, 2020). Específicamente en Colombia según la Contraloría General de la Nación, en su informe “Grandes hallazgos” refiere que la corrupción les cuesta a los colombianos al año 50 billones de pesos, que representan unos $US 18.400 millones.

Aunque las consecuencias económicas del fraude son evidentes, este no es el único impacto que genera sobre las empresas y la sociedad. La delincuencia económica también afecta seriamente la reputación de las organizaciones, la cultura de integridad y la salud mental de sus víctimas.

Una afectación a la reputación de las empresas puede afectar la continuidad del negocio al hacerlo insostenible en el tiempo, ya que afecta la confianza de sus clientes, proveedores e incluso de sus mismos empleados, pues preferirían comprar o trabajar en compañías mejor protegidas.

KPMG (2022) manifiesta que el 58% de su muestra encuestada reconoce haber sufrido una pérdida económica por fraude cibernético, el 20% señalan daños a su reputación y el 32% debió asumir investigaciones por incumplimiento.

En este mismo sentido, Andrés Gordón, líder mundial de servicios forenses e integridad de EY afirma que *"el cambio repentino y tectónico crea oportunidades para un comportamiento poco ético, incluido el fraude y la corrupción"*. Como lo evidencia el informe global de integridad 2022 (EY) el 55% de los encuestados expresa que los estándares de integridad se estancaron o empeoraron en los últimos 18 meses.

Así mismo, en la 17.ª edición del Informe de riesgos globales 2022 publicado por el Foro Económico Mundial, se refiere que *"los riesgos intangibles, como la desinformación, el fraude y la falta de seguridad digital, también afectarán la confianza pública"*. Señalando que el delito cibernético no solo alcanzará pérdidas de cientos de millones de dólares, sino que adicional ocasionará serios daños a la infraestructura crítica de las organizaciones, la cohesión social y el bienestar mental de sus víctimas.

Como se pudo evidenciar, el fraude seguirá siendo una amenaza latente que evoluciona y se trasforma a la misma velocidad que el mundo va cambiando, siempre nos lleva un paso adelante; lo que se ve reflejado en consecuencias devastadoras para las empresas y la sociedad en general.

La gestión antifraude como un proceso transversal

Para los empresarios de cualquier industria es necesario combatir el fraude ya que impacta negativamente la reputación y la economía de sus organizaciones

y del país. Por esto una adecuada gestión antifraude no solo evita tales pérdidas, sino que genera mejores condiciones de mercado.

Para esto es indispensable contar con un esquema antifraude completo y actualizado, que permita hacer frente a la realidad actual del fraude y que ayude a mitigar su impacto significativamente. Desde la experiencia del Instituto Nacional de Investigación y Prevención de Fraude, INIF, para la adecuada implementación de un esquema antifraude es indispensable que la compañía cuente con documentos que soporten las estrategias de prevención, detección y respuesta al fraude, a través de sus manuales de procedimientos, código de ética y reglas de conducta que enmarquen los conceptos de una cultura antifraude en la organización.

Para iniciar este esquema debe contar con una **prevención** efectiva que permita tomar las medidas necesarias y desarrollar habilidades encaminadas a minimizar el riesgo de fraude antes de su comisión.

Ernst & Young (EY) en su publicación, "Prosperando con integridad en la nueva normalidad: Perspectiva forense 2021", recalca la importancia de renovar las investigaciones y complementar con soluciones tecnológicas adecuadas que den respuesta los desafíos actuales de fraude y corrupción en un mundo socialmente distanciado.

Por esto en esta fase de **prevención** se hace necesario:

1. **Implementar técnicas analíticas, machine learning e inteligencia artificial:**: según la experiencia de INIF, a partir de los cruces de información y la perfilación de los clientes de las compañías, es posible detectar indicadores o señales de alerta en personas o procesos presuntamente fraudulentos.

La perfilación del defraudador se basa en la ponderación de diferentes características creadas a partir de fuentes externas e internas de información, en la cual se determina la probabilidad de que una persona esté conectada con casos de fraude.

Gracias a la ciencia de datos, es posible anticipar el riesgo de fraude asociado a una persona u organización, optimizando los recursos necesarios para el análisis de casos y el conocimiento integral de clientes, proveedores y terceros involucrados en los procesos estratégicos de las compañías.

De esta forma se maximiza el poder de los datos. La información que se recoge es un insumo poderoso para anticiparte a la comisión de fraude gracias al desarrollo de modelos analíticos y la combinación de estos con las reglas de negocio que darán como resultado una efectiva prevención de fraude.

2. **Desarrollar espacios de formación, sensibilización y capacitación** antifraude: El conocimiento es el arma más poderosa en la lucha contra el fraude, por esto se hace necesario crear espacios de formación especializada que contribuya a la prevención, detección y respuesta al fraude, aportando políticas, modelos, desarrollos y pautas que permitan a los interesados combatir este fenómeno, promoviendo con ello la elaboración de estrategias de control y fomentando una cultura organizacional transparente e íntegra. De esta forma, la gestión antifraude será parte del ADN de la compañía y los colaboradores estarán orientados hacia la prevención y detección temprana.

3. **Llevar a cabo procesos de selección y control del personal a la vanguardia:** Hacer uso nuevas herramientas y estrategias de evaluación que integren la tecnología avanzada, haciendo estos procesos más rápidos y minimizando cada vez más la probabilidad de error. De esta forma se mejorará la seguridad organizacional al prevenir el riesgo de fraude interno a través de la construcción de equipo de trabajo íntegros en todos los niveles de la organización.

Por su parte, una vez que el fraude se ha materializado en una organización es imprescindible **detectarlo** y neutralizarlo a tiempo de modo que se minimice el impacto sobre la compañía.

Para ello es necesario desarrollar metodologías especializadas e implementar herramientas tecnológicas que permitan aclarar los hechos, identificar oportunamente a los responsables y establecer mecanismos de control apropiados.

Por esto en esta fase de **detección** se hace necesario:

1. **Utilizar metodologías y técnicas avanzadas de investigación:** Obtener una mirada integral del fraude logrando una detección efectiva y oportuna por medio de un equipo de trabajo interdisciplinario que analice cada caso desde diferentes perspectivas con una mirada objetiva y realizar cruces de

información para analizar los casos en contexto y no como eventos aislados. Cada investigación es diferente, por lo cual es importante perfeccionar las herramientas y las metodologías sofisticadas de acuerdo con el objetivo de cada organización.

2. **Hacer uso de las redes sociales como fuente de información:** desde la experiencia de INIF esta es una de las estrategias de investigación más efectivas en la actualidad, ya que permite asociar patrones comunes, realizar cruces de información y visualizar comportamientos anómalos que se presenten en los procesos de las compañías, identificando las personas, los sucesos, las conexiones y los patrones clave que, de otro modo, podrían perderse.

3. **Responder efectivamente ante el fraude:** es necesario que todas las empresas y ciudadanos reporten el fraude tan pronto lo identifican, mediante los diferentes canales de denuncia existentes, de esta forma se podrán identificar los delincuentes y organizaciones criminales; además, de evitar sanciones normativas por incumplimiento.

¿Sabes reportar un fraude y cuáles son los canales?

- En Colombia puedes denunciar a través de las dos entidades oficiales: La policía Nacional y la Fiscalía General de la Nación. A través del sistema de denuncia virtual ¡ADenunciar! Que opera las 24 horas del día, los 7 días de la semana, los 365 días del año.
- También puedes reportar a través Línea Ética de INIF, un mecanismo de comunicación que te permite reportar de manera confidencial y anónima irregularidades o situaciones atípicas que hubieses identificado en tu compañía o en cualquier otro ámbito.

De igual forma, es necesario que la organización tome medidas contundentes que evidencien la cero tolerancia frente a este tipo de comportamientos o situaciones, promoviendo una cultura integra y estableciendo nuevas estrategias de prevención que mitiguen la probabilidad que el fraude se repita.

4. **Buscar y seleccionar la estrategia legal apropiada para lograr la judicialización:** INIF en estos casos procede a realizar un análisis jurídico de la documentación existente y del patrimonio probatorio con el que se pueda soportar una denuncia penal.

Para finalizar, es importante recalcar que la mejor estrategia de lucha contra el fraude es que todos nos sumemos y contribuyamos con nuestras acciones a la construcción de una cultura más íntegra y honesta alrededor del mundo.

"La articulación de esfuerzos entre autoridades y empresarios, es una fórmula exitosa para generar entornos económicos seguros, vincúlese al Frente de Seguridad Empresarial de la Policía Nacional y haga parte de esta importante estrategia de prevención".

Mayor Sonia Reyes Sánchez
Jefe Frente de Seguridad Empresarial DIJIN

APOYA:

BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE

Lic. PS.
CARLOS R. ARIZA
Magister en Criminologia

ORGANIZACIÓN G.D.C.
GESTIÓN, DESARROLLO Y CRECIMIENTO EMPRESARIAL

Grupo OET

icontec

INIF

RISKS INTERNATIONAL S.A.S.
"Trabajamos para facilitar decisiones seguras"

Táctica Empresarial

FRENTE DE SEGURIDAD EMPRESARIAL

CULTURA DE SEGURIDAD EN EL SECTOR EMPRESARIAL

2022

ISBN: 978-958-98894-9-7