Guía de Seguridad para los actores de la Cadena de Suministro

Herramienta práctica para la prevención criminal

V Edición

REPÚBLICA DE COLOMBIA
POLICÍA NACIONAL
DIOS Y PATRIA

POR UNA COLOMBIA
SEGURA Y EN PAZ

V Edición

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

Guía de Seguridad para los Actores de la Cadena de Suministro

Herramienta práctica para la prevención criminal

2016

TABLA DE AUTORES

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

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

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

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

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

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

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

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

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

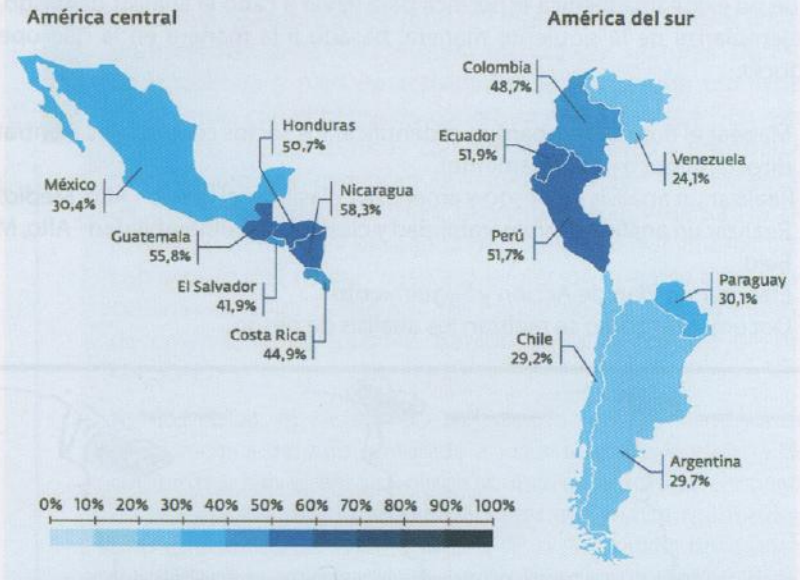
Además, se hace imperativo establecer un sistema que permita cerrar los ciclos, documentando e investigando los incidentes que hayan ocasionado efectos negativos, compartiendo y estudiando la casuística para conocer tendencias, nuevas modalidades y, lo más importante, divulgar las lecciones aprendidas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

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

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

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

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



Empresas afectadas por infecciones de malware (por país).

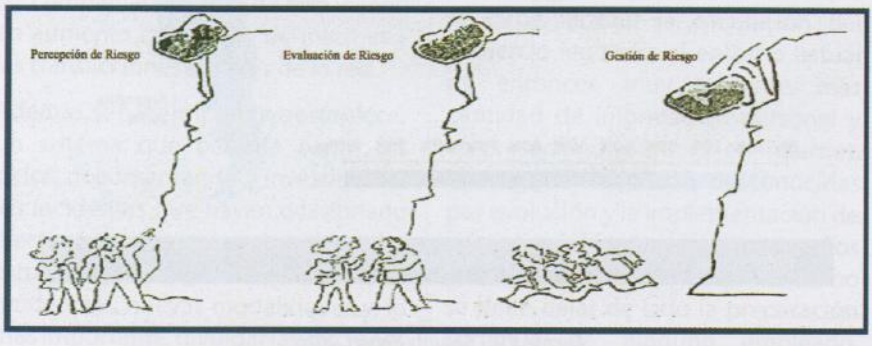
Fuente: ESET Security Report, 2016.

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

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

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

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



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

Aristides Contreras Fernández, Orlando Hernández Angarita
Directivos Comunidad latinoamericana de consultores y asesores en Gestión de riesgo y seguridad, COLADCA

ISBN 978-958-98894-6-6

OXY

Fasecolda
Federación de Aseguradores Colombianos

BASC