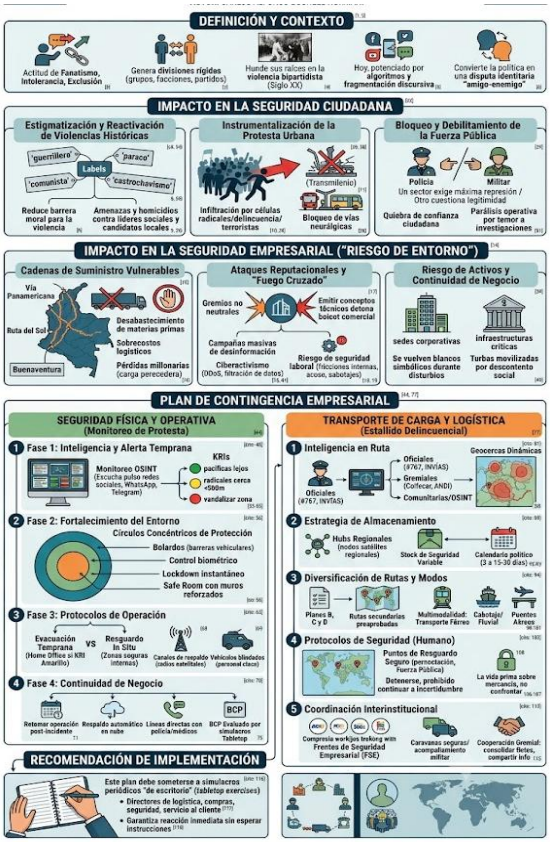


SECTARISMO POLÍTICO Y SU IMPACTO DE LA SEGURIDAD CIUDADANA Y EMPRESARIAL EN COLOMBIA

MONITOREO, ACCIONES Y PLAN DE CONTINGENCIA ANTE ATAQUES DELINCUENCIALES Y TERRORISTAS

COMPARTE: CARLOS ALFONSO BOSHELL NORMAN (CCO®)-(PPE®)

El sectarismo político es la actitud de fanatismo, intolerancia y exclusión hacia quienes piensan distinto dentro de un sistema político, genera divisiones rígidas entre familia, grupos, facciones, partidos y la sociedad. Se caracteriza por la defensa intransigente de una ideología y la descalificación de los adversarios como enemigos irreconciliables.

En Colombia no es un fenómeno nuevo; hunde sus raíces en la violencia bipartidista de mediados del siglo XX. Sin embargo, su versión contemporánea, potenciada por los algoritmos de las redes sociales y la fragmentación discursiva, ha transformado la polarización ideológica en un problema crítico de **orden público y seguridad empresarial**. Cuando la política deja de ser un espacio de debate técnico y se convierte en una disputa identitaria de tipo "amigo-enemigo", las métricas de riesgo en las ciudades y en los balances de las empresas se alteran profundamente.

La violencia de baja Intensidad que inicialmente presenta en la Seguridad Ciudadana en el plano urbano y rural a partir del sectarismo político actúa como un legitimador de la agresión y un catalizador del crimen organizado. Donde la reconfiguración de la violencia local tiende a revivir etiquetas históricas del conflicto armado colombiano (calificar al opositor de "guerrillero", "paraco" o "comunista"). En regiones vulnerables y periferias urbanas, esta estigmatización reduce la barrera moral para la violencia, convirtiéndose en un factor directo de amenaza y homicidio contra líderes comunitarios, reclamantes de tierras y candidatos locales.

La Instrumentalización y radicalización de la protesta, producto de una indignación impulsada por narrativas sectarias, facilita que las movilizaciones ciudadanas legítimas sean infiltradas o instrumentalizadas por células radicales o redes de delincuencia común y hasta terrorista. El resultado son afectaciones severas a la infraestructura pública de las capitales, como la destrucción sistemática de

estaciones de transporte masivo (Transmilenio, MIO, Transmetro, entre otros) y bloqueos de vías urbanas que desbordan la capacidad de la Policía.

Ante la desconfianza y parálisis institucional, el debate sectario sitúa de manera permanente a las Fuerzas Militares y a la Policía Nacional en el centro de la disputa política. Al debilitar la legitimidad institucional desde extremos opuestos (unos acusándolos de inacción y otros de represión desmedid), se quiebra la confianza ciudadana necesaria para los frentes de seguridad local, lo que es aprovechado por bandas criminales para copar espacios del multicrimen.

El Auge del "Riesgo de Entorno", producto del Sectarismo político en el sector corporativo, tiene implicaciones que van mucho más allá de la polarización de opiniones que impactan directamente la resiliencia y la continuidad del negocio. La vulnerabilidad crónica en las cadenas de suministro, el sectarismo facilita el uso del bloqueo de vías de hecho (como en la Vía Panamericana, la Ruta del Sol o los accesos a Buenaventura) como el principal mecanismo de extorsión y presión hacia el Gobierno central. Para las empresas, esto se traduce en desabastecimiento de materias primas, sobrecostos logísticos impredecibles y pérdidas millonarias por carga perecedera atrapada en carreteras.
Los ataques reputacionales y "Fuego Cruzado" digital, donde las empresas y los gremios económicos en Colombia ya no son actores neutrales ante los ojos de los sectores radicalizados. Emitir conceptos técnicos sobre reformas laborales, tributarias o de salud puede desencadenar campañas masivas de desinformación, llamados al boicot comercial o ataques de ciberactivismo (DDoS o filtración de datos) diseñados para castigar a la marca por su supuesta afiliación política, las fricciones internas y el riesgo de seguridad laboral, permea la cultura organizacional.

La polarización extrema entre los colaboradores dentro de una misma empresa o institución puede desencadenar problemas de acoso laboral, sabotajes operativos menores o la fuga de información sensible corporativa (amenazas internas) motivada por revanchismo ideológico contra las directivas de la empresa.

La gestión del riesgo corporativo en el país ha tenido que migrar de la vigilancia perimetral tradicional hacia la **inteligencia de entorno**. Hoy en día, la resiliencia de una operación depende de su neutralidad política activa, del monitoreo preventivo de fuentes abiertas (OSINT) para anticipar bloqueos viales y de la diversificación logística multimodal (uso de redes férreas, cabotaje o HUBS de almacenamiento satélites fuera de las ciudades principales).

Impacto en la Seguridad Ciudadana en Colombia

La radicalización del debate político deteriora la seguridad en las calles debido a tres fenómenos principales:

La estigmatización y reactivación de violencias históricas en Colombia a partir de la polarización tiende a encasillar los debates bajo viejas lógicas del conflicto armado (etiquetando posturas como "castrochavismo" o "paramilitarismo", entre otros). Tratando de deshumaniza al opositor y, en regiones vulnerables, traduce la diferencia política en violencia física o amenazas directas contra líderes sociales, defensores de derechos humanos y opositores locales.

La Instrumentalización de la protesta urbana a partir de la polarización genera una narrativa de "todo o nada". Cuando se convocan movilizaciones (tanto de oposición como de gobierno), el discurso radicalizado debilita el espacio para la manifestación pacífica. Esto facilita que células radicales o de delincuencia común instrumentalicen el descontento, provocando disturbios como bloqueos de vías neurálgicas (vandalismo en sistemas de transporte) que paralizan la seguridad de las ciudades.

El bloqueo y debilitamiento de la Fuerza Pública como resultado de un debate político polarizado suele poner a las autoridades de seguridadpública en el centro de la disputa ideológica. Mientras un sector exige máxima represión, otro cuestiona la legitimidad de cualquier acción de autoridad. Esto genera parálisis operativa por temor a investigaciones o, por el contrario, desconfianza civil legítima, rompiendo el binomio ciudadanía-policía que es clave para combatir el crimen común.

Impacto en la Seguridad Empresarial

La polarización política actúa como un catalizador que acelera y magnifica los conflictos locales, transformando tensiones latentes en incidentes de violencia real, donde los discursos de odio y la deshumanización del "adversario" político o social reducen la barrera psicológica para la agresión. Discusiones que inician en hilos de plataforma digitales especialmente que terminan escalando a agresiones físicas en las calles o eventos públicos.

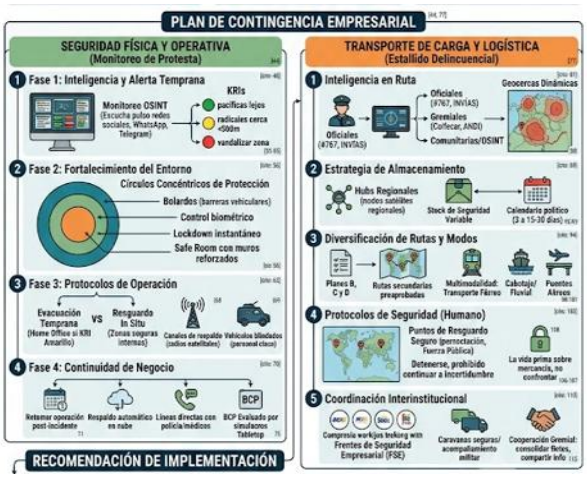
La difusión de desinformación masiva (noticias falsas) mina la legitimidad de las fuerzas del orden y el sistema judicial. Cuando la ciudadanía percibe a las autoridades como actores sesgados o enemigos, se reduce la denuncia del delito y aumenta la justicia por mano propia. La volatilidad en el espacio público propiciadas en las redes sociales permite la convocatoria y movilización ultra rápida de masas. Sin embargo, bajo un clima polarizado, marchas pacíficas son fácilmente infiltradas o radicalizadas por narrativas extremas en tiempo real, desbordando la capacidad de respuesta de la seguridad pública que, para la sociedad y las empresas, la polarización cambia las reglas del juego en la gestión de riesgos, obligando a los encargados de seguridad y resiliencia a monitorear variables que antes se consideraban ajenas a la operación.

Los Riesgo de Activos y Continuidad de Negocio en las empresas e infraestructuras críticas (bancos, cadenas de suministro, sedes corporativas, entre otras) a menudo

se convierten en blancos simbólicos durante disturbios civiles motivados ideológicamente. La seguridad física ya no solo se enfrenta a la delincuencia común, sino a turbas movilizadas por el descontento social. Las organizaciones quedan atrapadas en fuegos cruzados ideológicos. No alinearse con una causa —o hacerlo de manera percibida como tibia— puede desencadenar campañas masivas de boicot, doxxing (filtración de datos privados) contra ejecutivos, o ataques cibernéticos (como ataques DDoS) perpetrados por grupos de hacktivistas, pueden ser consecuencias.

Se presenta un desafío estratégico que la seguridad contemporánea ya no puede limitarse a colocar barreras físicas o sistemas de videovigilancia. Hoy en día, la inteligencia de fuentes abiertas (OSINT) y el monitoreo de la temperatura social en entornos físicos y digitales son herramientas indispensables para anticipar riesgos, proteger a las personas y garantizar la continuidad de las operaciones frente a un entorno social cada vez más fragmentado.

MONITOREO Y ACCIONES PREVIO DE LA PROTESTA SOCIAL QUE PUEDE DERIVAR EN ATAQUES DELINCUENCIALES Y TERRORISTAS



Antes de poner en marcha un plan de contingencia, la seguridad física empresarial debe estar ajustada para cumplir con sus objetivos principales que son la protección de personas, activos, ante disturbios delincuenciales, el enfoque tradicional de "reaccionar cuando el problema llega a la puerta" ya no es suficiente. Hoy en día, la clave está en la anticipación y la resiliencia estructural.

Un plan efectivo frente a este tipo de crisis se divide en cuatro fases críticas:

Fase 1: Inteligencia y Alerta Temprana (Prevención)
Antes de que una turba se concentre, la crisis ya se ha gestado en el entorno, la seguridad moderna empieza con la información.

- Monitoreo OSINT (Inteligencia de Fuentes Abiertas): Implementar herramientas para escuchar el pulso de las redes sociales, foros locales y canales de mensajería (Telegram, WhatsApp) donde se coordinan movilizaciones. Busca palabras clave relacionadas con tu sector, tu marca o las calles aledañas a tus instalaciones.
- Matriz de Indicadores de Riesgo (KRI): Define umbrales claros. Por ejemplo:
  Nivel Verde: Convocatorias a marchas pacíficas lejos de la instalación.
  Nivel Amarillo: Consignas radicales en redes, rutas de marcha que pasan a menos de 500 metros, o menciones indirectas a la empresa.

Nivel Rojo: Convocatoria explícita a bloquear o vandalizar la zona, o disturbios activos en las inmediaciones.

Fase 2: Fortalecimiento del Entorno (Seguridad Física Pasiva)
El diseño del espacio debe retrasar el acceso no autorizado el tiempo suficiente para que las fuerzas del orden respondan o el personal evacúe.

Principio de Círculos Concéntricos de Protección:

- **Perímetro Exterior:** Barreras vehiculares (bolardos) para evitar ataques con automóviles. Cortinas metálicas enrollables microperforadas en fachadas de vidrio (permiten ver hacia afuera, pero impiden el paso de piedras o proyectiles).
- **Perímetro Medio (Accesos):** Sistemas de control de acceso biométrico o por tarjeta que puedan ser bloqueados globalmente (lockdown) instantáneamente desde el centro de control.
- **Perímetro Interior:** Creación de una "Zona Segura" o Safe Room dentro del edificio, con muros reforzados, puertas blindadas y sistemas de ventilación independientes (en caso de uso de gases lacrimógenos en el exterior).

Fase 3: Protocolos de Operación y Protección del Personal (Seguridad Activa)
Los activos se pueden reemplazar; las vidas humanas no. El plan debe priorizar la integridad del equipo.

Protocolo de Evacuación Temprana vs. Resguardo In Situ:

- Si los KRI activan el Nivel Amarillo, la política debe ser el Home Office preventivo o la evacuación escalonada antes de que el transporte público o las vías colapsen.
- Si el disturbio estalla de forma sorpresiva, la orden debe ser el resguardo en las zonas internas seguras, alejando a todo el personal de ventanas y fachadas de vidrio.
- **Comunicaciones de Emergencia:** Disponer de canales de respaldo (radios satelitales o aplicaciones de comunicación cifrada que funcionen con bajo ancho de banda) por si las redes celulares se saturan o son inhibidas.
- **Protección de Dignatarios y Ejecutivos:** Rutas de escape alternativas y vehículos blindados listos para evacuar al personal clave si la empresa es el blanco específico de la protesta.

Fase 4: Continuidad de Negocio y Post-Incidente (Resiliencia)
Una vez que el disturbio cesa, el objetivo es retomar la operación lo antes posible minimizando las pérdidas.

- **Respaldo de Información y Sistemas:** Asegurar que los servidores locales tengan redundancia en la nube de manera automática. Si la planta física sufre daños o cortes de energía, los datos críticos deben estar a salvo.

- **Coordinación de Enlaces de Emergencia:** Mantener líneas directas preestablecidas con la policía local, empresas de seguridad privada colindantes (esquemas de seguridad compartida de la zona) y servicios médicos.
- **Plan de Continuidad de Negocio (BCP):** Cada paso del plan de contingencia debe ser evaluado mediante simulacros de mesa (tabletop exercises) con el comité de crisis de la empresa. El personal de seguridad física debe saber exactamente quién tiene la autoridad legal para ordenar el cierre total de las instalaciones en cuestión de segundos.

PLAN DE CONTINGENCIA ANTE UN POSIBLE ESTALLIDO SOCIAL QUE DERIBAN EN ACCIONES DELINCUENCIALES Y TERRORISTAS

Para diseñar un plan de contingencia efectivo para la cadena de suministro y en especial para el transporte de carga en Colombia, se debe partir de una realidad geográfica y operativa compleja: el país depende de corredores viales neurálgicos sumamente vulnerables (como la Vía Panamericana, el corredor Buenaventura-Cali, la Troncal del Caribe o la Ruta del Sol) donde un solo bloqueo puede fracturar el abastecimiento nacional.

Frente a bloqueos viales crónicos y disturbios derivados de la coyuntura social y política, la estrategia logística debe transitar de un modelo Just-in-Time (justo a tiempo) a uno de Resiliencia Activa. A continuación, se detallan los pilares para estructurar este plan:

Inteligencia en Ruta y Monitoreo Temprano

El activo más valioso cuando estalla un bloqueo es el tiempo de reacción. Un camión detenido en medio de una protesta es un activo atrapado y en riesgo.

Fuentes de información integradas: El centro de control de seguridad y /o monitoreo debe cruzar datos en tiempo real de tres niveles:

- Oficiales: Reportes de la Policía de Tránsito y Transporte (#767), el Instituto Nacional de Vías (INVÍAS) y el Ministerio de Transporte.
- Gremiales: Alertas de la Federación Colombiana de Transportadores de Carga (Colfecar), la Asociación Nacional de Empresarios de Colombia (ANDI) o Defencarga, entre otros.
- Comunitarias y OSINT: Monitoreo de emisoras radiales locales, cuentas regionales de X (Twitter) y grupos de apoyo en WhatsApp/Telegram de redes de transportadores, que suelen reportar "vías de hecho" horas antes de que se oficialicen.
- Geocercas Dinámicas: Configurar el sistema GPS de la flota para emitir alertas automáticas si un vehículo se aproxima a un punto crítico con disturbios activos (ej. zonas recurrentes como el Puente de Juanchito en Cali, el sector de El Bordo en el Cauca o los peajes de la Ruta del Sol).

Estrategia de Almacenamiento y Redundancia de Inventarios

Ante bloqueos crónicos que pueden durar días o semanas, la capacidad física de almacenamiento determina la supervivencia operativa de la empresa.

- Centros de Distribución Avanzados (Hubs Regionales): En lugar de centralizar todo el inventario en las grandes capitales (Bogotá, Medellín o Cali), se deben establecer nodos de almacenamiento satélite en regiones estratégicas fuera de los perímetros urbanos conflictivos.
- Política de "Stock de Seguridad" Variable: Incrementar los inventarios de materias primas críticas o productos de alta rotación basándose en el calendario político o social (ej. épocas de negociaciones de pliegos de peticiones, aniversarios de movilizaciones o debates de reformas clave). Pasar de un stock de 3 días a uno de 15 o 30 días antes de que inicien los periodos de alta conflictividad.

Diversificación de Rutas y Modos de Transporte (Plan B, C y D)

Un plan de contingencia robusto exige tener preaprobadas alternativas de transporte que no dependan exclusivamente de la red vial principal.

- Rutas alternas validadas: Mapear y auditar previamente rutas secundarias o terciarias. Aunque estas vías aumenten los costos de combustible y los tiempos de viaje (e incrementen el desgaste de los vehículos), permiten mantener el flujo de mercancía cuando las troncales principales están totalmente cerradas.

Multimodalidad:

- **Transporte Férreo:** Evaluar el uso de corredores activos (como la red férrea del Atlántico para conectar el interior con los puertos del Caribe) que suelen verse menos afectados por bloqueos civiles que las carreteras.
- **Cabotaje y Transporte Fluvial:** Utilizar el Río Magdalena o rutas marítimas de cabotaje (ej. Buenaventura - Tumaco o Cartagena - Turbo) para saltar bloqueos terrestres críticos.
- **Puentes Aéreos de Emergencia:** Mantener convenios previos con aerolíneas de carga para el envío exclusivo de insumos críticos o de alto valor que no puedan detenerse.

Protocolos de Seguridad y Gestión del Factor Humano

La prioridad absoluta del plan debe ser la integridad de las personas y la seguridad de las instalaciones y la carga ante posibles actos de vandalismo.

- **Puntos de Resguardo Seguro (Pernoctación):** Mapear estaciones de servicio, paradores camioneros o bases de la Fuerza Pública a lo largo de las rutas que cuenten con infraestructura de seguridad (cerramientos, cámaras, vigilancia privada). Si se detecta un bloqueo adelante, el conductor

tiene la instrucción estricta de detenerse en el punto de resguardo más cercano, prohibiendo continuar la marcha a zonas de incertidumbre.

- **Procedimientos frente a "Asonadas" o Saqueos:** Capacitar a los conductores bajo la premisa de que la vida prima sobre la mercancía. El conductor no debe confrontar a manifestantes ni intentar romper bloqueos por la fuerza. El vehículo debe contar con cerraduras de alta seguridad, marchas con precintos electrónicos y sistemas de apagado remoto en caso de que el camión sea tomado por terceros.
- **Pólizas de Seguro Especializadas:** Verificar que los contratos de transporte incluyan coberturas específicas contra terrorismo, asonada, motín, conmoción civil o huelga (pólizas lucrativas y de daño emergente debido a disturbios políticos), asegurando que los deducibles y topes estén actualizados a los valores reales de la carga.

Coordinación y Cooperación Interinstitucional

En Colombia, la seguridad en cadena de suministro es un esfuerzo colectivo. Ninguna empresa puede resolver un problema de orden público de manera aislada.

- **Frentes de Seguridad Empresarial (FSE):** Participar activamente en los frentes de seguridad coordinados por la Policía Nacional. Esto permite mantener una línea directa con los comandos departamentales para coordinar, cuando la situación lo permita, caravanas seguras o acompañamientos militares en tramos viales afectados.
- **Esquemas de Cooperación Gremial:** Aliarse con competidores o empresas del mismo sector logístico en la región para compartir información sobre el estado de las vías, unificar capacidades de almacenamiento de emergencia o negociar fletes consolidados en momentos de escasez de transporte.

Para concluir hay que estar preparados para cualquier escenario que se pueda presentar. Todos los planes deben someterse a simulacros periódicos, involucrando a los directores de seguridad, logística, compras y servicio al cliente. Esto garantiza que, ante el primer reporte de afectación a la seguridad, cada área de la compañía sepa exactamente cómo reaccionar sin necesidad de esperar instrucciones de la alta gerencia.

Feliz día

CARLOS ALFONSO BOSHELL NORMAN
CRIMINALISTA E INVESTIGADOR CRIMINAL
(CCO®) Certified Compliance Officer.
(PPE®) Professional Polygraph Examiner
CEL. +57 318 883 23 76
Correo: gerencia@cbconsultoresprofesionales.com
www.cbconsultoresprofesionales.com