AMERICAN CHAMBER MEXICO

Recomendaciones del Comité de Seguridad de AMCHAM 2024

Para abordar las áreas críticas de inseguridad identificadas en el Sondeo de Seguridad Empresarial 2024 y fortalecer la seguridad y el Estado de Derecho en México, es indispensable avanzar en:

1. **Mayor vinculación de la autoridad con el sector privado:** La participación e involucramiento de la iniciativa privada en el diseño, implementación y evaluación de las estrategias de seguridad de las autoridades federales, estatales y municipales es vital para enfrentar la delincuencia en México. La colaboración estrecha y efectiva entre ambos sectores puede mejorar la capacidad de respuesta ante amenazas y fomentar una comunicación constante y transparente.
2. **Capacitación y profesionalización:** Continuar y expandir la capacitación a los cuerpos policiales de los tres niveles de gobierno, enfocándose en la gestión de crisis y el uso de tecnología avanzada en seguridad.

Para ello, recomendamos implementar y perfeccionar las métricas de desempeño para la fuerza pública y fiscales basadas en el análisis de datos, incluyendo indicadores de eficiencia en la integración de carpetas de investigación y sentencia.

3. **Vigilancia y protección del autotransporte de mercancías:** Mejorar y actualizar los mecanismos de vigilancia para "blindar" las cadenas de suministro.

a. **Implementar corredores seguros** como una estrategia que permita fortalecer las acciones de inspección, seguridad y vigilancia por parte de la Guardia Nacional (GN) en las principales carreteras que conectan puertos y cruces fronterizos para el comercio binacional, así como las de mayor incidencia delictiva. Los corredores seguros también pueden ser una herramienta para asegurar la integridad de las cargas durante su trayecto;

El corredor seguro deberá contar con las siguientes características:

- **Vigilancia y monitoreo**: Inversión en infraestructura, tecnología y herramientas tales como arcos de seguridad, cámaras de video vigilancia, drones y tecnología en los filtros de control en las zonas de mayor incidencia delictiva, quedando a cargo de su vigilancia la Dirección General de Seguridad en Carreteras e Instalaciones de la Guardia Nacional.
- **Presencia de seguridad:** patrullas de la Guardia Nacional, puestos de control para inspección de vehículos y la **designación de un enlace de Guardia Nacional por regiones** a fin de agilizar el auxilio en casos de robo, secuestro o extorsión de empleados de las empresas, así como sobre las unidades y mercancías.
- **Alertas de seguridad:** Sistemas de alerta que notifiquen a las autoridades y a los operadores de cualquier anomalía o amenaza detectada.

- **Infraestructura:** mejoras en las vías y señalización adecuada.
- **Comunicación:** Establecer canales seguros y ágiles de cruce de información entre las autoridades y el personal de seguridad de las empresas, manteniendo en todo momento la confidencialidad de la información.
- **Protocolos de emergencia:** Establecer detallados protocolos nacionales de actuación de robo al autotransporte y homologar los criterios de operación en los tres niveles de gobierno.
- **Mantenimiento:** Involucrar a empresas privadas en la planificación y mantenimiento del corredor seguro.

b. Implementar paraderos seguros que garanticen la seguridad de todos los usuarios de las vías generales de comunicación que deseen descansar, abastecerse de combustible, tomar alimentos, e inclusive atención médica o mecánica. Por lo anterior, se deben de establecer acciones de coordinación entre la DGAF[1] – GN – CAPUFE[2] y concesionarios de autopistas, para la ubicación de estos espacios físicos.

Los paradores seguros deberán de contar por lo menos con las siguientes características:

- Estacionamiento
- Gasolinera
- Restaurante o alimentos
- Sanitarios con duchas y agua potable
- Mecánico
- Enfermería o primeros auxilios
- Acceso a internet (wifi público) y tomas de corriente para recargar celulares y otro tipo de dispositivos.
- Teléfono público con directorio de emergencias o red de comunicación para que los conductores puedan mantenerse en contacto con sus empresas y autoridades.
- Área de descanso cómoda y segura para que los operadores la usen sin necesidad que dormiten en la cabina.
- Supervisión continua de las operaciones del paradero para identificar y corregir cualquier vulnerabilidad.
- Puesto de patrullaje de la Guardia Nacional.

c. Generar mecanismos de divulgación del operativo Escalón, paraderos seguros y de corredores seguros y **contar con informes de medición de resultados** para promover el uso del mecanismo con más transportistas.

[1] Dirección General de Autotransporte Federal, Secretaría de Infraestructura, Comunicaciones y Transportes
[2] Caminos y Puentes Federales, Secretaría de Infraestructura, Comunicaciones y Transportes

d. **Asignar al Registro Público Vehicular los recursos humanos, tecnológicos y financieros requeridos.** Dado que esta entidad opera bajo la jurisdicción del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, la dotación de estos recursos se convierte en un paso clave para asegurar su operación eficiente en la prevención y seguimiento de delitos relacionados con vehículos de carga.

e. Establecer con la autoridad federal una **ventanilla única de reporte de robo de vehículos** que facilite su seguimiento y recuperación y evitar que posteriormente puedan ser usados para robo al transporte en carreteras u otros delitos de alto impacto. La ventanilla deberá garantizar la atención al robo sin importar la jurisdicción por entidad federativa, por lo que se debe garantizar que todas las autoridades correspondientes formen parte de la ventanilla.

f. Solicitar a la Fiscalía General de la República el **establecimiento de un procedimiento ágil, eficiente, simplificado, transparente**, y que unifique criterios para la **devolución y liberación de las unidades vehiculares objeto del delito**.

g. **Reforma al Código Nacional de Procedimientos Penales** a fin de que en materia de robo de autotransporte, las unidades y mercancías recuperadas sean resguardadas en las instalaciones de las empresas ofendidas o tener áreas específicas, adecuadas y autorizadas para su resguardo.

h. **Colaboración interinstitucional** para la localización de los puntos de venta de la mercancía robada en zonas urbanas.

4. **Estrategia Nacional de Ciberseguridad (ENCI):** En conjunto con el Comité de Innovación y TICs de AmCham, recomendamos actualizar e implementar la ENCI con la participación del sector privado, académico y la sociedad civil en su diseño, desarrollo y ejecución, bajo la tutela de las siguientes recomendaciones:

a. **Fases para su desarrollo:** Iniciación, Inventario y análisis, Producción, Ejecución, y Seguimiento y evaluación.

- **Iniciación:** establecer a una autoridad, existente o nueva, como responsable.La autoridad a cargo de la coordinación e implementación de la ENCI debe contar con facultades y atribuciones suficientes para enfrentar los desafíos, por ello, es indispensable que exista una clara asignación de responsabilidades y canales efectivos de coordinación y comunicación entre autoridades federales y locales.
- **Inventario y análisis:** conocer y evaluar el presente y futuro del panorama nacional de la ciberseguridad, con el fin de obtener información trazable y auditable para la elaboración de la estrategia.

- **Producción:** creación del texto de la estrategia, con la participación del sector público, privado y de la sociedad civil por medio de consultas públicas y grupos de trabajo, que culminan con la publicación y obligatoriedad de los compromisos.
- **Ejecución:** observación y desarrollo de la estrategia trazada.
- **Seguimiento y evaluación:** acción gubernamental para asegurar que la estrategia cumple con su finalidad. Determinar si es óptima con base en el análisis de la evaluación de riesgos.

b. Derechos Humanos y protección de la seguridad nacional. La ENCI deberá tener un enfoque en los Derechos Humanos, puesto que el uso y acceso a medios electrónicos e internet ha evolucionado hasta convertirse en un Derecho Humano. Asimismo, deberá ser una política pública vinculada a la protección de la seguridad nacional, al ser parte fundamental del funcionamiento óptimo de la infraestructura crítica del Estado.

c. Regulación conforme al TMEC y Cooperación trilateral: La ENCI debe tomar en cuenta las disposiciones del Capítulo 19 del TMEC en la materia y acelerar la creación de un mapa de ruta para impulsar estándares y políticas de ciberseguridad en un marco intersectorial que sea mundialmente reconocido y que se centre en identificar y gestionar riesgos. Asimismo:

- **Establecer un foro trilateral permanente** para la participación de diversos sectores interesados en ciberseguridad, en donde las partes interesadas participen de manera activa para (i) lograr la armonización de políticas; (ii) promover los principios establecidos en el TMEC; y (iii) combatir las amenazas cibernéticas de una manera conjunta.
- **Acordar una taxonomía común entre México, EE.UU. y Canadá.** El lenguaje utilizado para describir la ciberseguridad actualmente no es consistente, lo que obstaculiza la colaboración intersectorial y transfronteriza. La falta de un lenguaje común aumenta el desafío de la gestión de riesgos cibernéticos, en especial, para aquellas organizaciones que operan en diversos países o que integran cadenas de suministro a nivel global.
- **Creación de un programa trilateral** para el desarrollo de capacidades de ciberseguridad, en especial para las PyMEs.

d. Gestión de Riesgos: se deben establecer protocolos, mecanismos y herramientas que formen parte de la ENCI como:

- Protocolo nacional para compartir información: Protocolo de ataques cibernéticos que establezca esquemas de colaboración entre autoridades, organizaciones, empresas y usuarios. Se debe garantizar la confidencialidad de la información de las víctimas de los ciberataques para evitar afectaciones a la reputación.

- Boletín público, periódico e informativo de los riesgos y eventos cibernéticos que publique la autoridad coordinadora. Es importante, para la estrategia de prevención, conocer los ataques perpetrados y potenciales afectados.
- Generar estadísticas oficiales con datos que provengan de instituciones públicas y privadas de los tipos de riesgos, incluyendo lugares, periodicidad e incidencia.
- Realizar simulacros de ciberseguridad guiados por expertos en la materia a fin de acelerar los procesos de respuesta y ciberresiliencia.

e. Marco regulatorio: También es necesario la creación de un marco regulatorio integral basado en la gestión de riesgos que sea flexible para adaptarse a la evolución tecnológica.

f. Procuración de Justicia: Es necesario la creación y fortalecimiento de fiscalías especializadas y capacitar a las y los impartidores de justicia en ciberseguridad y TICs.

- Creación de fiscalías especializadas en delitos cibernéticos en los fueros federal, local y militar, de acuerdo con sus competencias, mismas que se podrán definir en las leyes orgánicas de las fiscalías, así como en la normatividad que regula a los cuerpos policiacos.
- Establecer jueces especializados en el ámbito cibernético, a nivel federal y estatal. Se requiere capacitar a las y los jueces que conocerán los casos relacionados a ciberseguridad, ciberdelincuencia, ciberdelitos y funcionamiento de las TIC.

5. **Colaboración bilateral entre México y EEUU para fortalecer la seguridad fronteriza**: Generar programas de coordinación de vigilancia y control entre las autoridades de ambos países para reducir el tráfico de armas, trata de personas y migración ilegal asociada a la delincuencia, etc.;
6. **Generar lineamientos precisos para el tratamiento de la información confidencial relacionada con los delitos de robo, extorsiones y fraudes**, así como con las víctimas, testigos y el procedimiento penal para reducir al máximo los riesgos de seguridad de las víctimas, testigos y pérdida de evidencias para el proceso criminal;
7. **Blindaje del sistema financiero**: Fortalecer el sistema financiero contra el lavado de dinero mediante el uso de tecnologías avanzadas y la capacitación especializada del personal. Implementar sistemas de alerta temprana y monitoreo continuo de transacciones sospechosas. Incentivar el uso de inteligencia financiera en las investigaciones, utilizando datos sobre ingresos ilegales obtenidos por la venta de productos robados y otros delitos.

Por su parte, es imprescindible que el sector privado replique las mejores prácticas identificadas a lo largo de los años en esta materia, algunos ejemplos de ellas son:

1. **Cultura de Seguridad Corporativa**: Impulsar la cultura de la seguridad corporativa con un documento rector que se base en tres ejes: i) prevención de riesgos, ii) manejo de crisis y iii) continuidad de negocio.
2. **Cadena de Suministros:** Mantener un padrón actualizado de transportistas y robustecer la confiabilidad de los operadores mediante pruebas de poligrafía, toxicología y evaluaciones técnicas.
3. **Análisis de Riesgo en carreteras:** Analizar permanentemente el panorama de riesgo a nivel de carreteras y ajustar las rutas estratégicas en función de los hallazgos, utilizando datos actualizados y tecnología de mapeo.
4. **Inversión en Tecnologías de Seguridad.** Realizar una evaluación integral de los riesgos y necesidades específicas de la empresa en materia de seguridad e identificar áreas vulnerables y potenciales amenazas para priorizar inversiones, en:

a. Innovación y tecnología (CCTV, controles de acceso y sistemas de alarma y detección;

b. Planes de gestión de crisis;

c. Medidas de ciberseguridad;

d. Capacitación especializada de los equipos internos

Los resultados del sondeo reflejan los retos y las adaptaciones que las empresas han adoptado en un entorno de seguridad complejo y en evolución en México. A pesar de las preocupaciones, las empresas han demostrado resiliencia y proactividad al implementar tecnologías avanzadas, sistemas de gestión de crisis y medidas preventivas. La inversión en innovación y tecnología ha sido crucial para mejorar la seguridad interna y demostrar un compromiso constante con la protección de sus operaciones.

Es crucial que el gobierno refuerce la vigilancia, combata la corrupción y mejore la coordinación entre instancias para responder efectivamente a estos desafíos y fortalecer la confianza del sector empresarial en las instituciones de seguridad. Con un enfoque en la prevención y el fortalecimiento de las capacidades locales de seguridad, junto con la colaboración entre empresas y autoridades, México puede avanzar hacia un entorno más seguro y próspero para las empresas y sus colaboradores.

Consulta el **10° Sondeo de Seguridad** de **AMCHAM** de **aquí**.

Contacto: Gerardo Arana | garana@amcham.org.mx