



Fecha: 08 de Octubre 2026.
Salón Terraza, Hacienda de los Morales.
Asistentes: 171.
Patrocinador: Ford Pro.

Durante el desayuno mensual de octubre, el Lic. Rubén Fajardo Correa, CPP, PSP, PCI, expuso ante los profesionales de seguridad de ASIS Capítulo México 217 un panorama claro y contundente: el crimen organizado ya no solo opera en la calle, hoy ataca directamente a las empresas, a sus activos, a sus personas y a su capacidad de operar. El mensaje central de la ponencia fue que las corporaciones deben dejar de ver al crimen organizado como un problema de seguridad pública ajeno y entenderlo como un riesgo corporativo estratégico, que combina violencia, tecnología y corrupción.

1. Ataques con Inteligencia Artificial: Fraude y Robo de Información. La IA se ha convertido en una herramienta criminal. Los grupos delincuenciales la utilizan para: Fraude sofisticado: Creación de deepfakes de voz y video para suplantar a directivos y ordenar transferencias bancarias, con voces clonadas de CEOs y directores financieros. Phishing hiperpersonalizado: Correos y mensajes generados por IA que copian el estilo de la empresa, con datos reales robados de LinkedIn y redes sociales. Robo de información y tecnología: Exfiltración de datos sensibles, propiedad intelectual, secretos industriales y bases de datos de clientes, para su venta o extorsión posterior.

Automatización del delito: Bots que atacan sistemas de forma masiva, buscando vulnerabilidades 24/7. La consecuencia no es solo económica: es pérdida de confianza, daño reputacional y sanciones legales por fuga de datos.

2. Extorsión Personal y Empresarial. La extorsión ha escalado de nivel. Ya no es solo telefónica. Extorsión empresarial: Exigencia de pagos mensuales para permitir operar, amenazas de cierre de operaciones, sabotaje o ataques a infraestructura. Extorsión personal: Amenazas directas a ejecutivos, gerentes y sus familias, con vigilancia previa y conocimiento de rutinas. Ransomware y ciber-extorsión: Secuestro de sistemas operativos. La empresa debe pagar para recuperar su información y continuar operando. Extorsión digital interna: Uso de información robada de empleados para chantajearlos y convertirlos en colaboradores internos. El riesgo se traslada del patrimonio a la integridad física y psicológica del personal.

3. Derecho de Piso y Derecho de Paso. Dos de las amenazas más graves para la operación en territorio: Derecho de piso: Cobro ilegal por "permitir" que la empresa opere en una zona, abra una sucursal, tienda o planta. Se convierte en un impuesto criminal permanente. Derecho de paso: Cobro por transitar por rutas,

carreteras o caminos controlados por el crimen. Afecta directamente a la logística, transporte de mercancía, distribución y cadena de suministro. Ambos esquemas incrementan costos, interrumpen operaciones y obligan a las empresas a modificar rutas, horarios y zonas de operación, afectando su competitividad.

4. **Gobernanza Criminal.** El crimen organizado busca controlar el territorio no solo con violencia, sino con gobernanza criminal: Impone reglas, horarios y castigos en comunidades donde opera. Sustituye al Estado en la resolución de conflictos. Infiltra gobiernos locales, policías y proveedores. Establece redes de “protección” y lealtad con la población. Para las empresas, esto significa operar bajo dos autoridades: la legal y la criminal, con riesgo de colusión involuntaria, lavado de dinero y responsabilidad legal.

Conclusiones y recomendaciones para la empresa

El Lic. Fajardo Correa concluyó que la respuesta debe ser integral, no solo guardias y cámaras:

1. **Inteligencia corporativa:** Monitorear el entorno, las rutas y las amenazas regionales.
2. **Cultura de ciberseguridad:** Capacitar a empleados contra IA, fraude y phishing, con políticas de doble verificación para transferencias.
3. **Protección ejecutiva:** Planes de protección para directivos y sus familias, con gestión de información personal.
4. **Resiliencia operativa:** Protocolos contra extorsión y ransomware, con respaldo de información fuera de línea y planes de continuidad.
5. **Cumplimiento y debida diligencia:** Verificación de proveedores, contratistas y socios para evitar infiltración criminal.

Mensaje final

El crimen organizado está evolucionando más rápido que las empresas. La seguridad corporativa debe pasar de ser reactiva a ser preventiva, con estrategia, tecnología y personal capacitado.

