PERSPECTIVAS | SEGURIDAD CORPORATIVA



DE LA INVESTIGACIÓN A LA ANTICIPACIÓN

Cómo transformar la Seguridad Corporativa mediante el análisis de procesos y el modelo CSPAM

Por Julio Marval

La seguridad corporativa está evolucionando. Ya no es suficiente investigar los incidentes después de que ocurren: las organizaciones necesitan identificar las vulnerabilidades de sus procesos, anticipar conductas irregulares y diseñar controles capaces de prevenir, detectar y aportar evidencia.

CORPORATE SECURITY • INVESTIGATIONS • LOSS PREVENTION • RISK MANAGEMENT

El desafío de una nueva Seguridad Corporativa

Durante décadas, buena parte de la función de Seguridad Corporativa ha estado orientada a responder ante incidentes: investigar fraudes, esclarecer pérdidas patrimoniales, identificar responsables y documentar incumplimientos. Sin embargo, existe una pregunta que los profesionales de seguridad debemos comenzar a formular con mayor frecuencia: ¿por qué nuestros procesos permitieron que el incidente ocurriera?

La experiencia en organizaciones de sectores como petróleo y gas, industria automotriz, consumo masivo, tabaco y bebidas demuestra que muchos eventos de pérdida no comienzan necesariamente con una conducta deliberada. En ocasiones, se originan en debilidades operativas, excepciones no controladas, supervisiones insuficientes o decisiones humanas sin trazabilidad.

Cuando estas condiciones se repiten sin consecuencias, una oportunidad de error puede convertirse en una oportunidad de abuso. El desafío consiste en pasar de una seguridad reactiva a una seguridad anticipativa.

CSPAM: una metodología para analizar los procesos

A partir de esta necesidad desarrollé el Corporate Security Process Analysis Model (CSPAM), un modelo de análisis orientado a identificar vulnerabilidades, fortalecer los controles y mejorar la capacidad de detección de irregularidades dentro de los procesos organizacionales.

El modelo se estructura sobre tres dimensiones fundamentales:

1. **Prevención.** Identificar dónde pueden producirse las desviaciones antes de que generen pérdidas. Esto requiere comprender los procesos, sus responsables, los niveles de autorización y las oportunidades de intervención humana.
2. **Detectabilidad.** Determinar qué capacidad tiene la organización para identificar una irregularidad, quién puede detectarla y cuánto tiempo podría permanecer inadvertida. Un riesgo de alto impacto y baja detectabilidad representa una prioridad.
3. **Evidencia.** Asegurar que los controles produzcan registros verificables. Las aprobaciones trazables, los registros de actividad, las marcas de tiempo y el versionado documental permiten reconstruir decisiones y respaldar investigaciones.

Un control que no deja evidencia verificable puede resultar insuficiente cuando la organización necesita demostrar qué ocurrió.

Tres capas para llevar el modelo a la práctica

La aplicación del CSPAM requiere un abordaje sistemático que conecte el conocimiento del negocio con la evaluación del riesgo y el diseño de controles:

- Comprensión del proceso. Analizar compras, inventarios, nómina, gastos, accesos, devoluciones, gestión de terceros y conflictos de interés. El propósito es mapear el flujo, sus responsables y los puntos de decisión humana.
- Análisis del riesgo y detectabilidad. Identificar puntos vulnerables, excepciones recurrentes y mecanismos de supervisión existentes. La pregunta central es cómo, cuándo y por quién podría detectarse una desviación.
- Diseño de controles. Establecer mecanismos preventivos, detectivos y probatorios, con responsabilidades y trazabilidad claramente definidas.

El objetivo no es multiplicar controles burocráticos, sino desarrollar controles inteligentes que reduzcan oportunidades de pérdida y mejoren la eficiencia operativa.

La información que ya tiene la organización

Una de las mayores oportunidades para Seguridad Corporativa está en aprovechar información que habitualmente ya existe en las organizaciones. Los reportes operativos, las estadísticas y las métricas de la cadena de suministro pueden revelar patrones que no son evidentes cuando cada evento se analiza de manera aislada.

- Excepciones reiteradas por una misma persona.
- Aprobaciones realizadas fuera de los horarios habituales.
- Modificaciones posteriores al cierre de operaciones.
- Expedientes con documentación incompleta.
- Movimientos de inventario que requieren análisis frente a los objetivos comerciales.
- Reiteración de desviaciones en determinados proveedores o procesos.

La combinación de estas variables permite pasar de la observación aislada al análisis de patrones y tendencias. Aquí la tecnología, la analítica de datos y la automatización pueden convertirse en grandes aliados de la prevención.

Gobernanza: Seguridad Corporativa como integrador

Ninguna metodología será sostenible si depende exclusivamente del departamento de Seguridad. El CSPAM propone fortalecer la coordinación mediante tres instancias de gobernanza:

Comité de Prevención y Control de Pérdidas: orientado a identificar vulnerabilidades y desarrollar acciones preventivas.

Comité de Toma de Decisiones: responsable de evaluar situaciones relevantes, definir prioridades y establecer medidas correctivas.

Comité de Seguimiento y Monitoreo: encargado de verificar compromisos, medir resultados y asegurar la continuidad de las acciones.

La Dirección General debe respaldar esta estructura, mientras Seguridad Corporativa actúa como integrador entre las distintas áreas del negocio.

El profesional de seguridad que necesitan las organizaciones

La evolución de nuestra profesión exige nuevas competencias. El profesional de Seguridad Corporativa debe comprender el negocio, conocer sus procesos, interpretar indicadores, gestionar riesgos y participar en decisiones estratégicas.

Investigar sigue siendo fundamental, pero anticipar dónde puede ocurrir una pérdida, identificar por qué los controles podrían fallar y proponer soluciones sostenibles representa un salto cualitativo en nuestra contribución empresarial.

La seguridad deja de ser únicamente una función de protección para convertirse también en una herramienta de eficiencia, gobernanza y continuidad del negocio.

Reflexión final

La madurez de una organización no debería medirse solamente por su capacidad de resolver incidentes, sino también por su capacidad de evitar que se repitan.

El futuro de la Seguridad Corporativa está en integrar investigación, prevención, tecnología, inteligencia y análisis de procesos.

No se trata solamente de investigar lo que ocurrió. Se trata de comprender cómo pudo ocurrir, identificar dónde podría repetirse y diseñar un sistema capaz de anticiparse.

SOBRE EL AUTOR

Julio Yran Marval

Profesional de Seguridad Corporativa con más de 20 años de experiencia internacional en operaciones de seguridad, investigaciones, prevención de pérdidas, gestión de crisis y protección de activos en América Latina.
Desarrollador del Corporate Security Process Analysis Model (CSPAM).

Corporate Security | Investigations | Loss Prevention | Risk Management