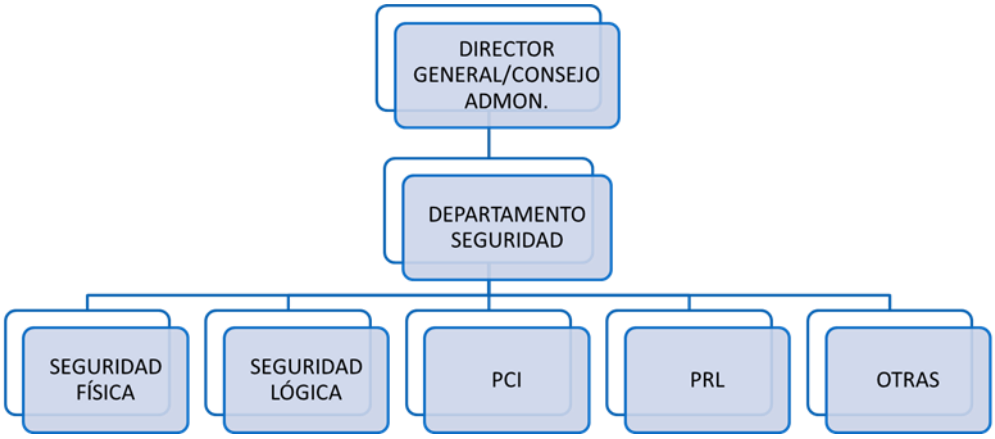
## TENDENCIAS DE GESTIÓN DE LA SEGURIDAD EN GRANDES CORPORACIONES

En la actualidad la organización y tendencia, tanto en el día a día como en el cumplimiento de sus objetivos futuros, de los departamentos de seguridad corporativos, se articula en base a las siguientes características:

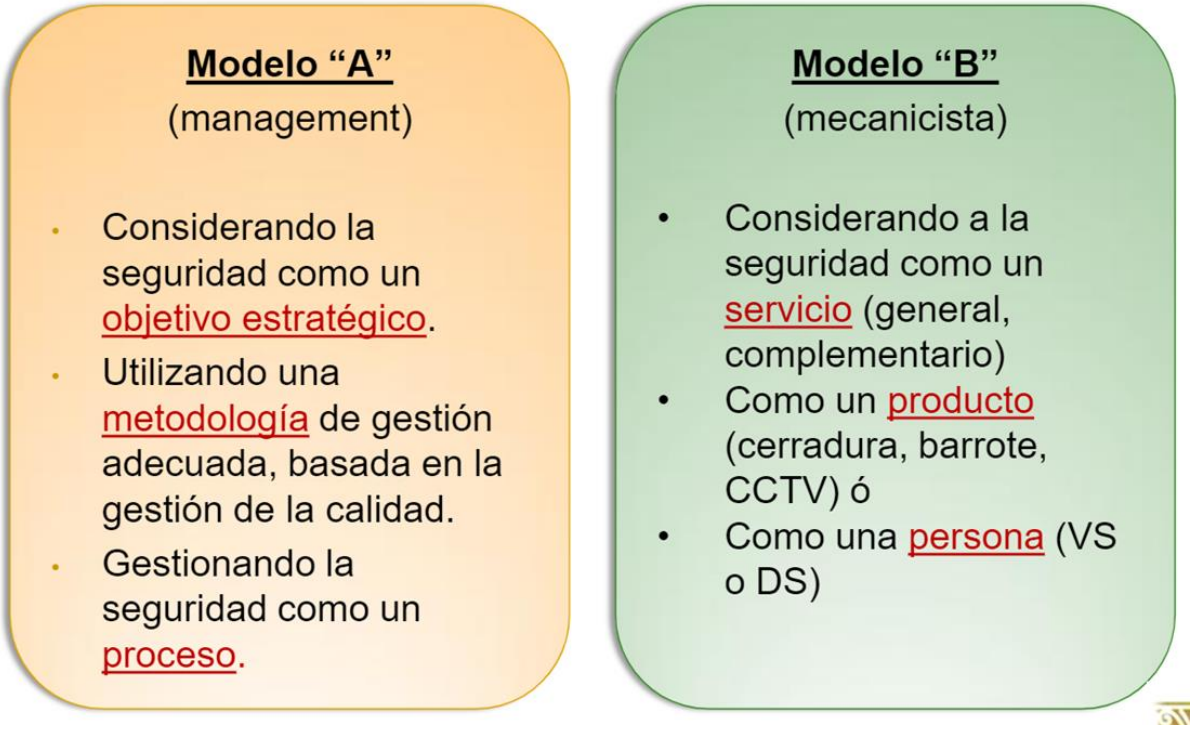
- **El director de seguridad como gestor de riesgos**: más allá de lo que la normativa nacional de seguridad privada establece entre sus funciones el director de seguridad se ha convertido, siguiendo el modelo anglosajón, en un gestor de los diferentes riesgos que pueden afectar a su corporación, aglutinando las diversas ramas de la seguridad integral. En ese modelo ideal de organización, que aún no es predominante entre las compañías, Seguridad depende de la Alta Dirección y todas las materias de seguridad dependen de ella.




*Fuente: elaboración propia*

- **La seguridad como proceso científico**: la seguridad no es un proceso aleatorio, ni una moda como parece darse con frecuencia hoy día en la instalación de sistemas, sino que es un proceso científico basado en la lógica; por eso es necesario un estudio detallado y un análisis de riesgos adecuado antes de implantar cualquier tipo de medidas; es por eso que la construcción del modelo debe girar en torno al director de seguridad como profesional reputado y de una alta cualificación, que debe ejercer un rol absolutamente basado en el liderazgo respecto de su equipo y del departamento que dirige, asumiendo responsabilidades y ejecutando la toma de decisiones.
- **Dependencia de la Alta Dirección**: el director del departamento de seguridad debe tener dependencia directa del más alto estamento ejecutivo de la compañía, debido a la criticidad para la empresa de las materias que son competencia de su departamento. El director de seguridad debe ser un elemento recurrente en las acciones de importancia de la compañía, adoptando una posición estratégica dentro de la misma.
- **Objetivos del departamento de seguridad en sintonía con los objetivos de la compañía:** el departamento de seguridad no debe ser una isla dentro de la organización, no puede hacer la guerra por su cuenta ni tener unos objetivos propios diferentes de los de la compañía. Los objetivos del departamento tienen que estar alineados con los de la corporación, ya que, como cualquier departamento de la compañía, sirve a los intereses de esta. Eso pasa por la necesidad imperiosa de conocer el negocio, tanto a nivel de sector como de funcionamiento interno de la propia empresa donde está encuadrado.

- **El Departamento de Seguridad como parte de la empresa**: seguridad es un Departamento más de la empresa y puede aportar valor diferencial a la organización (Modelo ESRM- Enterprise Security Risk management). Los directores de seguridad deben hablar el mismo lenguaje que el resto de los directivos para tener peso en el Comité de Dirección.
- **Evolución hacia un sistema de gestión**: paso de un modelo mecanicista, que considera a la seguridad como un servicio, producto o persona, hacia un **modelo de gestión** que considera **la seguridad como un proceso estratégico**, utilizando una **metodología** basada en la gestión de la calidad.




*Fuente: José Manuel García Diego*

- **Aprovechamiento de la tecnología**: el avance que supone la tecnología permite llegar más lejos y optimizar los recursos, reduciendo presupuestos.
- **Big data**: Tratamiento del dato como elemento esencial para conocer qué está pasando en tiempo real, y que apoya en la toma de decisiones y ayuda a justificarlas.

En la actualidad, respecto a los servicios de seguridad y lo que apuntábamos anteriormente, se dan las siguientes características:

- Tendencia generalizada a la disminución de servicios armados, excepto donde existe obligación legal y en las infraestructuras críticas.
- Importante disminución de los servicios de vigilancia puros tal y como venían concibiéndose tradicionalmente. Los avances tecnológicos permiten disminuir el elemento humano y, además, financieramente los medios técnicos pueden amortizarse; por tanto, nos encaminamos a un escenario en que se realiza una combinación de la tecnología con el recurso humano.

- En consonancia con lo anterior se está produciendo una transformación de la vigilancia en supervisión, realizando servicios en remoto y por otro lado dando servicio de respuesta concretas ante incidentes; como vemos hay disminución de los elementos humanos por un lado y una transformación de estos por otro, acompañados del respaldo técnico y de las posibilidades que permite la tecnología.
- Importancia de la especialización del director de seguridad como profesional cualificado y de su liderazgo en la gestión de los especialistas de su equipo como recurso.
- Conforme a las dos premisas anteriores, es imprescindible la adecuada formación en todos los niveles y particularmente en el ámbito tecnológico dentro de la vigilancia y en el ámbito del liderazgo en los directivos de seguridad.

Bajo mi punto de vista, en ese entorno cambiante se dan nuevas amenazas que nos obligan a buscar nuevas soluciones en materia de seguridad y de su gestión.

Entre las nuevas amenazas podemos señalar:

- Entorno VUCA: hace referencia a los términos en inglés: Volatility, Uncertainty, Complexity and Ambiguity. Volatilidad (volatility). En la realidad actual, sobre todo aplicado al entorno empresarial, es la velocidad a la que se puede producir una gran cantidad de cambio.
- Crisis: en la actualidad y tras la pandemia del Covid se está dando no sólo en el ámbito económico, sino también hay una crisis de valores, un choque cultural importante fruto de la globalización, y una crisis existencial en lo personal que está repercutiendo en el mercado laboral.
- Globalización: como señalábamos, para lo bueno y lo malo la globalización afecta y se globalizan también las amenazas (movimientos migratorios, delincuencia organizada transnacional, ciberdelincuencia…).
- Aumento de la delincuencia, como consecuencia de algunos de los factores señalados antes, que provocan y van a seguir provocando cada vez mayores disturbios sociales.
- Terrorismo Internacional, sigue estando presente, en particular el de etiología yihadista, con algunos pequeños repuntes locales.
- El ciberespacio como nuevo campo de juego para los delincuentes.

Estas nuevas amenazas nos obligan a nuevas soluciones, algunas de las cuales ya hemos señalado, y que podrían resumirse en:

- Tecnológicas: basadas en aprovechar los avances tecnológicos para implementar soluciones que incidan sobre los riesgos y optimicen costes.

- Digitalización: Obtención, recopilación y tratamiento del dato para la toma de decisiones. Permite conocer la situación en tiempo real y justificar las decisiones adoptadas.

- Normalización: Tendencia a certificación bajo estándares. Cada vez es más común el obtener certificaciones en normas internacionales; esto beneficia a la empresa y garantiza un determinado nivel de cumplimiento frente al estándar. Cobra aquí especial relevancia la del profesional de la gestión de la seguridad como experto que asesora en temas de consultoría y capaz de auditar competentemente tanto de forma interna como externa en las compañías; interesante figura, además como asesor externo de

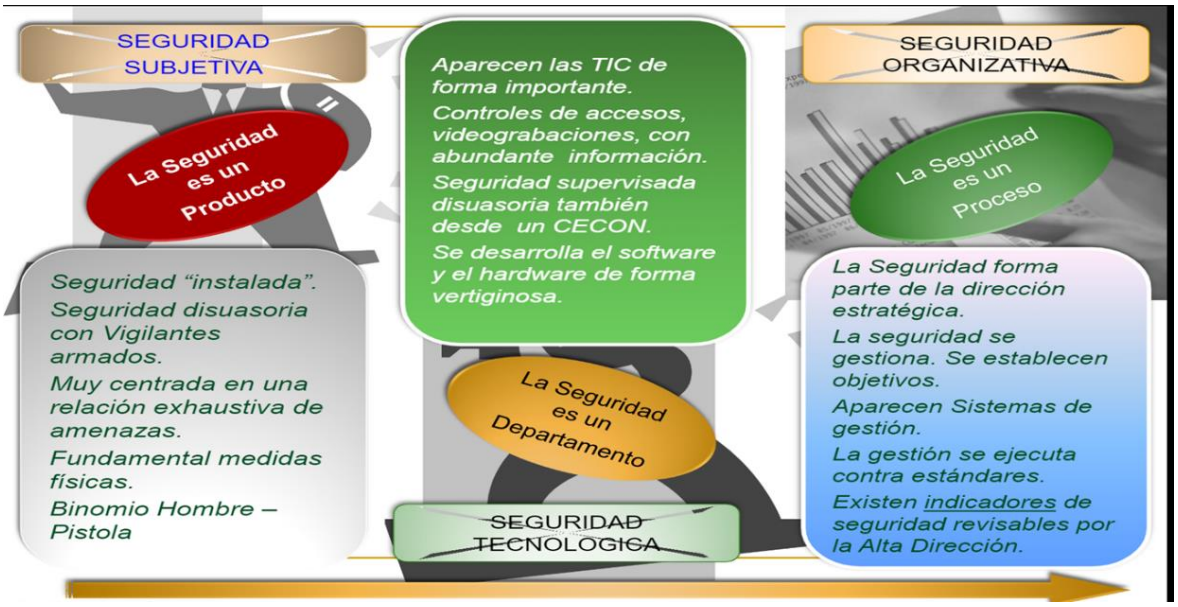
compañías sin departamento de seguridad o como figura “implant” en departamentos con pocos recursos humanos propios.

- Inteligencia, análisis, prospectiva: Se busca una seguridad predictiva frente a la tradicional seguridad “forense”. Buscamos la anticipación para la mejor gestión de riesgos entendidos de una forma global y poder contribuir al negocio.

- Seguridad Integral: todo ello bajo el enfoque de la convergencia de las seguridades en una única Seguridad, basada en el director de seguridad como figura fundamental que lidera y en el departamento de seguridad como eje fundamental de la gestión y el cambio, haciendo que la seguridad pase a ser un proceso estratégico para las compañías, bajo estándares y regidos por la eficacia y eficiencia en la consecución de resultados y totalmente alineados con los objetivos empresariales.

Podemos hablar de que el concepto de seguridad, y por ende el de su departamento, está en evolución continua; así, podemos señalar diferentes fases:

- En un primer momento podemos hablar de una seguridad subjetiva, en la que la seguridad es básicamente un producto. Es una seguridad eminentemente disuasoria, con vigilantes armados y predominio de las medidas de seguridad físicas, y muy centrada en una relación exhaustiva de amenazas.
- En un segundo momento, en el que nos encontraríamos en la actualidad de forma mayoritaria, hablamos de una seguridad tecnológica, en la que la seguridad se constituye como un departamento más. Es una seguridad marcada por la aparición de las TIC; se desarrollan de forma vertiginosa el hardware y el software. Es una seguridad en la que se implementan los sistemas de control de accesos, videograbaciones, etc., y hay abundancia de información; al mismo tiempo la seguridad sigue siendo disuasoria y supervisada desde centros de control.
- El escalón final, al que se debería tender, es aquel compuesto por una seguridad organizativa, en la que la seguridad se constituye como un proceso. Aquí, la seguridad forma parte de la dirección estratégica, que es siempre lo ideal. La seguridad se gestiona y se establecen objetivos. Aparecen los sistemas de gestión y esa gestión se ejecuta contra estándares. Existen indicadores de seguridad que pueden ser revisables por la alta dirección.




*Fuente: José Manuel García Diego*

Así pues, hay dos principales enfoques de la seguridad: administrar frente a gestionar. La mera administración no necesita de figuras especializadas, pero no aporta ningún valor a la organización. El ámbito de la gestión, sin embargo, hace referencia a llevar adelante una iniciativa o proyecto, e implica planificar, desarrollar, controlar y actuar.