Prioridades, retos y oportunidades en SST del **sector de la vigilancia en Colombia**





Marco García
Asesor internacional en SST
Director académico CONFEVIP / CEO de SGE S.A.S.

En Colombia, el sector de vigilancia y seguridad privada desempeña un papel crucial en la economía aportando, a 2023, cerca de 10,5 billones de pesos anuales, es decir, el 1,2 % del Producto Interno Bruto (PIB) y generando, a su vez, según la Superintendencia de Vigilancia y Seguridad de Colombia[1] 390.000 empleos formales que dan sustento al mismo número de familias.

En Colombia existen cerca de 1200 empresas de seguridad que incluyen cooperativas y empresas en todas sus modalidades siendo la fuente más importante de empleo formal del país. No obstante, el cálculo no tiene en cuenta a aproximadamente 1900 empresas informales y que se encuentran en proceso de legalización.

Lo más destacable del sector radica en la naturaleza de su misión: proteger preventivamente a la ciudadanía y sus bienes de la delincuencia.

Esta labor desempeña un papel crucial en el fortalecimiento del nivel de confianza tanto de inversionistas locales como extranjeros quienes desempeñan un papel fundamental como impulsores del desarrollo y la dinamización de la economía. A medida que la sociedad adquiere mayor seguridad,

[1] Entidad responsable de regulación y control de las empresas de seguridad privada en Colombia. *https://www.supervigilancia.gov.co/*

los empresarios se sienten más confiados para invertir en el país. En contraste, un alto grado de inseguridad resultaría en costos adicionales para las empresas, como pólizas y mayores inversiones para garantizar la seguridad de las operaciones, los activos y los trabajadores. Esto, a su vez, reduciría los rendimientos financieros y afectaría negativamente la viabilidad de su presencia en el mercado nacional.

"A nivel de Iberoamérica, el principal reto del sector de la seguridad es ser más productivo, pero generando entornos saludables para su personal que incluyan controles efectivos para su exposición al riesgo público, así como a los nuevos riesgos asociados a la transformación digital" fue una de las conclusiones más destacadas y aceptadas por los especialistas internacionales en temas de seguridad que participaron en el VI Congreso de Seguridad desarrollado en 2023 en Punta Cana, República Dominicana y organizado por la Confederación de Empresas de Seguridad Privada de Colombia (Confevip)[2].

En Latinoamérica, la sociedad se enfrenta a una situación de incertidumbre política y social, lo cual ha propiciado una transformación en el *modus operandi* de la delincuencia. Además, se han sumado nuevos actores, como los ciberdelincuentes, agravando aún más la complejidad de la situación.

Este escenario ha dado lugar a un mercado emergente para las empresas de seguridad, lo cual puede mejorar su productividad. Sin embargo, este crecimiento debe basarse en la adaptación a los nuevos riesgos asociados a estas transformaciones. Entre dichos riesgos se incluye la incorporación de la ciberseguridad como una preocupación pública, abarcando todos los delitos relacionados con la misma. Además, se observa un cambio en la valoración del riesgo psicosocial, con consecuencias potenciales derivadas de estos delitos.

En este contexto, elementos como la rotación de personal, los turnos de



La sociedad está experimentando grandes transformaciones, y los riesgos asociados a estos cambios también evolucionan, requiriendo una adaptación continua por parte de las empresas de seguridad y sus colaboradores".

trabajo y los mecanismos de contratación están experimentando cambios significativos con la digitalización y las nuevas tendencias laborales derivadas de la virtualización. Por ende, resulta fundamental que las empresas brinden formación a sus empleados en nuevas competencias digitales para que puedan mantenerse en el mercado laboral. La sociedad está experimentando grandes transformaciones, y los riesgos asociados a estos cambios también evolucionan, requiriendo una adaptación continua por parte de las empresas de seguridad y sus colaboradores.

Así las cosas y partiendo de la premisa objetiva de que las empresas de seguridad privada actualmente centran su servicio en un 95 % en la seguridad presencial (a través de guardas de seguridad) y solo un 5 % en tecnología (es decir, por medio de cámaras, video vigilancia, alarmas y drones), se requiere una gestión eficiente del personal como prioridad. La apuesta se centra en crear entornos saludables que proporcionen a los empleados una movilidad social segura sin comprometer su integridad personal, con la aspiración de incrementar la esperanza de vida y extender sus períodos productivos con el tiempo. En este sentido, las empresas ya están adaptándose para ofrecer condiciones

[2] Confevip es la Confederación de empresas de seguridad y vigilancia privada de Colombia.

laborales dignas, incluso, para poblaciones laborales mayores de 65 años.

La alta competencia que se da en la actualidad entre las empresas de seguridad —formalizadas y no formalizadas— asociadas a los requerimientos de licitaciones públicas y privadas les genera la necesidad de ser más competitivas. El factor diferencial lo impone la regulación pública y los pliegos privados donde los factores de calificación y desempates incluyen elementos de equidad e inclusión de personal joven, de la tercera edad, minorías étnicas y sociales, mujeres y personas en condición de discapacidad. La incorporación cada vez mayor de personal con estos atributos es un reto para las empresas que deben garantizar un entorno seguro para estos empleados y a su vez, implementar medidas que garanticen su bienestar y un control de riesgos efectivo. Esto incluye mejoras en su infraestructura física y actualizaciones de sus sistemas de gestión, así como de sus protocolos de actuación tanto operativa como funcional y administrativa.

Lo anterior está llevando a que algunos gremios de empresas de seguridad tengan convenios de inclusión laboral con el Estado colombiano, en especial, con la Alta Consejería Presidencial para la Equidad de la Mujer y la Alta Consejería Presidencial para los Derechos Humanos y el Derecho Internacional, alianzas que regularán la participación de las minorías y de población vulnerable en las empresas de seguridad y garantizará, de manera equitativa, el control de riesgos laborales por parte de las empresas por medio de seguimientos bipartitas periódicos de cumplimiento de los compromisos adquiridos

De otro lado, es indudable que la sociedad está cambiando a pasos agigantados con la llegada de la Revolución 4.0 que implica una transformación tecnológica y social en todos los niveles,





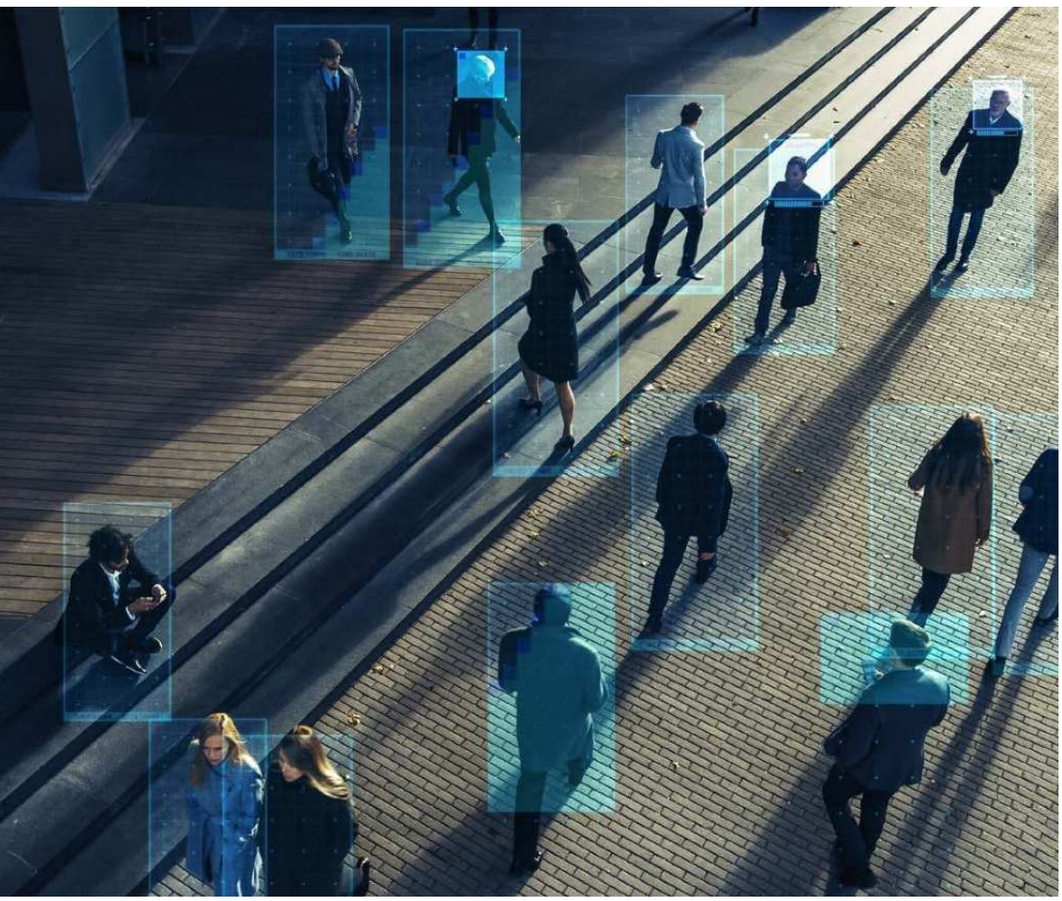
abarcando tanto el ámbito gubernamental como el empresarial, el social y el técnico. De hecho, la pandemia por la COVID-19 aceleró el uso de la tecnología en el ámbito laboral y personal, pero también desencadenó los riesgos asociados a la virtualización y la digitalización de los procesos, que incluyen cambios en la operación de los delincuentes la cual pasó de ser física a digital.

Este fenómeno tiene injerencia notable en el sector de la vigilancia. En este ámbito, se está incrementando la demanda de tecnología como una solución prioritaria para abordar problemas de seguridad que impulsa al sector a iniciar su transformación hacia este nuevo mercado. En este contexto, resulta crucial definir e implementar estrategias que prevengan eventos relacionados con los riesgos laborales emergentes en este entorno en evolución.

Con la transición de la seguridad presencial a un enfoque mixto que incorpora un componente tecnológico en

"Los riesgos laborales asociados a las empresas de seguridad han experimentado un cambio significativo con su actual transformación tecnológica".

crecimiento, la transformación de los perfiles laborales y las competencias del personal se hacen imprescindibles. La formación y capacitación en asuntos tecnológicos se convierte en un requisito indispensable para lograr la sostenibilidad, especialmente, si se considera la creciente tendencia mundial hacia la incorporación de soluciones de seguridad, como el uso de drones, guardas virtuales, cámaras de vigilancia con inteligencia artificial para reconocimiento facial, domótica, sistemas de alarma con notificaciones digitales y sistemas de acompañamiento de mercancías críticas mediante geoposicionamiento y videos en tiempo real, entre otras tecnologías emergentes.



La figura tradicional del guarda presencial está cambiando y las empresas, así como los potenciales empleados deben adaptarse rápidamente. El desafío radica en preservar el empleo y convertir al guarda de seguridad en un gestor tecnológico de seguridad. En este contexto, los empresarios tienen la oportunidad de capacitar a sus empleados actuales en las habilidades necesarias para enfrentar la nueva realidad. Este esfuerzo se vuelve aún más relevante cuando las organizaciones consideran la posibilidad de aumentar sus porcentajes de empleados mayores de 45 años para potenciar su competitividad.

Los riesgos laborales asociados a las empresas de seguridad han experimentado un cambio significativo con su actual transformación tecnológica. Este cambio se refleja en el nuevo espacio laboral, que ya no se limita solo al entorno físico, sino que también abarca el ámbito digital, con tareas llevadas a cabo en la virtualidad, en internet, la nube y, cada vez más, en el metaverso. Este entorno emergente conlleva una nueva generación de riesgos no solo en seguridad, sino también laborales, especialmente, los relacionados con la ciberseguridad y la protección de la información, los cuales, cada día, se hacen más evidentes y ganan mayor relevancia.

En el contexto colombiano, las empresas se ven confrontadas con la imperativa necesidad de establecer controles que resguarden tanto a su personal como a su información y activos ante las crecientes amenazas de delincuencia y ciberdelitos. Entre los riesgos más prominentes, se destacan el *pretexting*, que implica la creación de escenarios ficticios para persuadir

a las víctimas de revelar información confidencial; la extorsión telefónica con fines lucrativos; el *smishing*, que consiste en recibir mensajes de texto fraudulentos que simulan ser de entidades legítimas como redes sociales, bancos o instituciones públicas; el *vishing*, un engaño mediante el uso de voz; y el *pharming*, donde los delincuentes redirigen a los usuarios a sitios web falsos para obtener y sustraer información personal o financiera. Ante estos desafíos, la implementación de medidas preventivas se vuelve esencial para fortalecer la seguridad empresarial.

Según el boletín periódico del Centro Cibernético de la Policía Nacional, en 2023 se registraron más de 23 mil denuncias por ataques cibernéticos[3]. El informe resalta que los tres tipos de ciberataques más frecuentes fueron el hurto por medios informáticos con 9753 casos (experimentando un aumento del 5 % con respecto a 2022); la violación de datos personales con 4705 casos y una disminución del 9 %; así como el acceso abusivo a sistemas informáticos con 4610 casos que muestran una reducción del 6 % en comparación con el año anterior.

Estos delitos están teniendo un impacto significativo en la labor de las empresas de seguridad, las cuales se ven obligadas a reestructurar sus departamentos para incorporar servicios de ciberseguridad. Este escenario no solo impone el reto de manejar de manera efectiva los riesgos asociados al ámbito laboral, sino que también conlleva un aumento en los riesgos psicosociales derivados de estas nuevas condiciones.

La creciente presión generada por la amenaza constante de ciberdelitos contribuye al incremento de factores psicosociales adversos. El estrés y la incertidumbre relacionada con la continuidad laboral, causada por la inestabilidad y cambios constantes en las condiciones de trabajo, se han convertido en desafíos significativos para los empleados de estas empresas de seguridad. Es imperativo que las organizaciones no solo fortalezcan sus medidas de seguridad cibernética, sino que también implementen estrategias para mitigar los efectos psicológicos negativos en su personal, promoviendo un entorno laboral más saludable y resiliente.

La creciente presión generada por la amenaza constante de ciberdelitos contribuye al incremento de factores psicosociales adversos".



Esto implica la necesidad de adaptar los procedimientos de actuación y establecer controles sólidos que constituyan la base para la prevención de incidentes que puedan surgir.

Otro desafío y prioridad para la mayoría de las empresas en este sector es

[3] El Centro Cibernético de la Policía Nacional es la dependencia de la Dirección de Investigación Criminal e Interpol encargada de desarrollar estrategias y proyectos para la ciberseguridad, la ciberdefensa y la protección de la información y los datos que circulan por el ciberespacio de los habitantes en el territorio nacional. Más información en https://www.policia.gov.co/ciberseguridad

lograr un crecimiento sostenible en el actual ambiente de incertidumbre caracterizado por la inestabilidad regulatoria, la polarización y el inconformismo social, la debilidad a nivel de judicialización del delito cada vez más creciente y las condiciones cambiantes con alta fluctuación a nivel económico.

Para abordar este reto, el desarrollo e integración de sistemas de gestión es clave. Estos sistemas no solo proporcionan ventajas competitivas en el ámbito comercial, sino que también se traducen en la obtención de certificaciones en normativas como la ISO 9001, 45001, 14001, 27001 y 280004, y particularmente, en lo que concierne a este sector, la ISO 18788. Esta última norma es exclusiva para empresas de seguridad, centrando su enfoque en el cumplimiento de los Derechos Humanos como su pilar fundamental. Incluye un componente de gran relevancia que aborda el control del uso de la fuerza, el relacionamiento con los actores y los factores que determinan la evaluación y prevención de la materialización de riesgos públicos.

La visión desafiante en Salud y Seguridad en el Trabajo (SST) del Sector de Vigilancia —basada en las condiciones actuales y la evolución continua del mercado, la delincuencia, el entorno laboral y las nuevas necesidades de protección de la sociedad— se resume en la imperativa promoción y aplicación de estrategias efectivas hacia una prevención basada en la tecnología. Esto implica fomentar la conciencia y cultivar una sólida cultura en SST utilizando herramientas educativas y de sensibilización con tecnologías de vanguardia como realidad aumentada e Inteligencia Artificial (IA). Además, se busca mejorar la gestión de los nuevos riesgos laborales mediante la incorporación de sensores y dispositivos basados en Internet de las Cosas (IoT) en la prevención y el seguimiento, junto con la digitalización de todas las herramientas de gestión.

A medida que las empresas se transforman hacia un mundo cada vez más digital y virtual, las medidas de control de riesgos laborales deben evolucionar al mismo ritmo. Aunque representa un gran desafío, los beneficios significativos se visualizan a corto plazo.

Es imperativo que las organizaciones no solo fortalezcan sus medidas de seguridad cibernética, sino que también implementen estrategias para mitigar los efectos psicológicos negativos en su personal, promoviendo un entorno laboral más saludable y resiliente".



[4] ISO 14001: Sistemas de Gestión Ambiental.
ISO 45001: Sistemas de Gestión de la Seguridad y Salud en el Trabajo
ISO 9001: Sistemas de Gestión de la Calidad
ISO/IEC 27001: Sistemas de Gestión de la Seguridad de la Información - Requisitos.
ISO 28000: Sistemas de Gestión de la Seguridad para la Cadena de Suministro
ISO 18788: Sistemas de Gestión de Seguridad Privada