“La seguridad convergente es un requisito estratégico para las empresas”

Francis Cepero Tchernev CEO de Primion Technology

La integración de seguridad física, ciberseguridad y operaciones permite a las organizaciones anticipar riesgos, optimizar la gestión del personal y mejorar su eficiencia sin comprometer la continuidad del negocio.

Hoy, los entornos físicos y digitales están interconectados y la seguridad ya no puede abordarse por separado. La convergencia entre sistemas, la gestión eficiente del personal y la protección de infraestructuras críticas exigen una visión integrada. Para entender cómo afrontarlo, hablamos con Francis Cepero Tchernev, CEO de Primion Technology, compañía especializada en soluciones integradas de gestión de personal y seguridad que ayudan a mejorar la operativa, reforzar la protección y avanzar hacia un modelo de seguridad verdaderamente convergente.

En los últimos años se habla cada vez más de seguridad convergente. ¿Qué implica realmente este concepto y por qué se ha vuelto imprescindible para las organizaciones?

La seguridad convergente ha dejado de ser una tendencia para convertirse en un requisito estratégico. Significa integrar en un único marco operativo lo que antes funcionaba en silos: seguridad física, ciberseguridad y sistemas operacionales. En un entorno donde lo físico y lo digital se mezclan, las amenazas se desplazan entre ambos mundos y, si no hay alineación, la organización queda expuesta.

Este enfoque permite gestionar el riesgo de forma global, anticiparse y responder con una coordinación antes imposible. Un incidente puede empezar en una puerta, continuar en una red y terminar afectando a procesos críticos; por eso la convergencia es, además, un cambio cultural y organizativo.

También aporta eficiencia: al integrar sistemas, unificar datos y automatizar procesos, se gana agilidad, se reducen costes y se decide con información completa y en tiempo real. Quien adopta este modelo con visión estratégica opera con más resiliencia y en mejor posición para competir y crecer.

La gestión de operaciones y del personal (workforce operations) está ganando peso en entornos complejos. ¿Cómo ayuda la tecnología a optimizar estos procesos sin afectar a la operativa diaria?

El problema no es la falta de herramientas, sino la fragmentación: turnos, accesos, presencia o certificaciones suelen vivir en sistemas desconectados. La tecnología aporta valor cuando se integra y automatiza lo manual, reduciendo errores sin añadir fricción.

Si el sistema asigna turnos y permisos por rol, ubicación o cualificación y activa/desactiva accesos automáticamente, la operación gana agilidad y consistencia. Con datos en tiempo real se ajusta la planificación, se mejora la experiencia del empleado y se responde mejor a picos de demanda o imprevistos.

Integrada de forma coherente, la tecnología no interrumpe la operativa: la acelera, la ordena y la hace más precisa, reduciendo costes y reforzando tanto la resiliencia como la seguridad.

> “Integrada de forma coherente, la tecnología no interrumpe la operativa: la acelera, la ordena y la hace más precisa, reduciendo costes y reforzando la resiliencia”

¿Qué papel juega hoy el control de accesos dentro de una estrategia global de seguridad?

El control de accesos ya no es solo abrir o cerrar puertas: es el punto donde convergen identidad, operativa y protección de activos. Garantiza que cada persona esté donde debe, cuando corresponde y con la autorización adecuada.

En una estrategia global asegura cumplimiento y reduce riesgos en zonas sensibles, y además aporta inteligencia operativa (presencia, movimientos) para planificar mejor y reforzar la continuidad. También puede activar flujos de trabajo automáticamente, uniendo seguridad y eficiencia.

> “El control de accesos ya no es solo abrir o cerrar puertas: es el punto donde convergen identidad, operativa y protección de activos”

¿Cómo se integra hoy la seguridad física con otros sistemas y qué beneficios aporta esa visión más conectada?

Durante años, la seguridad física se gestionó en piezas aisladas (cámaras, accesos, alarmas). Integrarla hoy con otros sistemas permite correlacionar vídeo, accesos y actividad operativa para ganar contexto y velocidad de respuesta, además de habilitar protocolos coordinados y automatizados. Romper silos no es solo tecnología: es una decisión estratégica que mejora seguridad, eficiencia y prevención.

Los entornos industriales y las infraestructuras críticas incorporan cada vez más sistemas OT e IoT. ¿Cuáles son los principales riesgos en este contexto y cómo deben abordarse?

La convergencia IT/OT y el crecimiento de OT e IoT amplían la superficie de ataque y permiten que una amenaza salte de lo digital a lo físico y viceversa. Los riesgos clave son la falta de visibilidad de dispositivos y dependencias y una gestión débil de identidades y permisos; el impacto puede ser interrupción, daños y riesgos para las personas.

La respuesta pasa por segmentar sin perder coordinación, unificar identidades y accesos y supervisar eventos de forma continua. “Zero Trust” también aplica: cada acceso debe validarse en el plano físico y digital para asegurar continuidad y seguridad.

Con tantos sistemas, datos y tecnologías implicadas, la clave parece estar en la integración. ¿Qué retos encuentran las organizaciones a la hora de unificar todo este ecosistema y cómo pueden superarlos?

El principal reto es la heterogeneidad: años de soluciones puntuales, proveedores distintos y arquitecturas diferentes por centro o país. A esto se suma la falta de alineación entre IT, seguridad y operaciones y, a menudo, la ausencia de un modelo común de datos (identidades, roles, ubicaciones, activos).

Para superarlo hay que reducir complejidad con una plataforma unificada y basada en estándares, gobernanza clara y un modelo común de identidades y accesos. Empezar por procesos críticos acelera resultados.

En Primion lo vemos claro: la integración no es un proyecto técnico, es una decisión de negocio que mejora cómo una empresa opera, se protege y crece.

> “En Primion lo vemos claro: la integración no es un proyecto técnico, es una decisión de negocio que mejora cómo una empresa opera, se protege y crece”

www.primion.io

Primion forma parte del Grupo Azkoyen