TECNOLOGÍA DE **SEGURIDAD** OPERACIONAL

Principios, desafíos y cómo lograr resultados críticos para la misión utilizando OST

Un e-book de:

SIA
SECURITY INDUSTRY ASSOCIATION

Powered by: EXPO SEGURIDAD MÉXICO

Si quieres saber más sobre estas tendencias asiste a Expo Seguridad México este 2, 3 y 4 de junio, 2026

ALLEGION M.C. DEAN BUILDING INTELLIGENCE ONVIF wesco

RESUMEN

El informe de Tecnología de Seguridad Operacional (OST) de la Security Industry Association proporciona una guía integral para comprender, seleccionar, integrar y gestionar las tecnologías que sustentan la seguridad física moderna. Elaborado por expertos de la industria, el informe está diseñado para profesionales de seguridad, instaladores de sistemas, gerentes de negocio y usuarios finales que buscan tomar decisiones informadas sobre sus inversiones en seguridad.

PRINCIPIOS CLAVE

1. **Definición de OST:** OST se refiere a los elementos técnicos —hardware y software— que permiten a los profesionales de seguridad realizar su trabajo. Esto incluye sistemas que conectan, monitorean, gestionan y ejecutan operaciones de seguridad, cerrando la brecha entre el mundo físico y el digital.
2. **Convergencia:** El informe destaca la creciente convergencia entre la tecnología operacional (OT), la tecnología de la información (IT) y la seguridad física. Las estrategias de seguridad efectivas requieren colaboración y alineación técnica entre estos dominios.
3. **El contexto importa:** Las definiciones y requerimientos de OST dependen del contexto, variando según la industria, el tamaño de la organización y las necesidades específicas de seguridad.

PRINCIPALES CATEGORÍAS DE OST

El informe identifica cinco categorías principales de tecnología de seguridad operacional, cada una con sus propios componentes y desafíos:

- Sistemas de Control de Acceso Físico (PACS)
- Tarjetas de acceso, biometría, PIN, soluciones móviles y gestión de visitantes
- Sistemas de Videovigilancia
- CCTV, cámaras IR, PTZ, térmicas, corporales y de reconocimiento facial; analítica de video
- Sistemas de Detección (Alarmas y Sensores)
- Alarmas inteligentes, sensores de movimiento, sísmicos, humo/gas, ruptura de vidrio y ambientales
- Seguridad Perimetral y Ambiental
- BMS, energía de respaldo, barreras, cercas, iluminación, control de acceso vehicular y contención
- Gestión de Seguridad
- Centros de operaciones de seguridad, reportes de incidentes, notificación masiva, seguridad IoT y ciberseguridad

DESAFÍOS CLAVE

- **Integración e interoperabilidad:** Muchos componentes de OST no están diseñados para trabajar juntos, lo que genera dificultades de integración, silos de información e ineficiencias. Estos problemas pueden crear brechas de seguridad y aumentar la carga de trabajo manual.
- **Complejidad:** La diversidad de sistemas OST, frecuentemente provenientes de distintos fabricantes y generaciones, incrementa la complejidad en su implementación, mantenimiento y actualización.
- **Falsas alarmas:** Los sistemas de detección son propensos a falsas alarmas debido a errores humanos, mala instalación, tecnología obsoleta o factores ambientales, lo que puede generar complacencia y omisión de amenazas reales.
- **Migración a la nube:** El cambio hacia soluciones basadas en la nube ofrece escalabilidad, pero introduce nuevos desafíos en costos, especialización, cumplimiento normativo y dependencia de proveedores.
- **Gestión del ciclo de vida:** El éxito a largo plazo requiere planificar mantenimiento, actualizaciones, cumplimiento y evolución de amenazas, no solo la implementación inicial.

MEJORES PRÁCTICAS Y GUÍA ESTRATÉGICA

- **Definir objetivos claros:** Identificar los problemas específicos que OST debe resolver antes de evaluar soluciones.
- **Alineación de stakeholders:** Involucrar desde el inicio a todas las partes relevantes (IT, seguridad y líderes de negocio).
- **Matriz de requerimientos:** Utilizar un checklist de requerimientos funcionales y no funcionales alineados con los objetivos del negocio.

- **Pruebas piloto:** Realizar pruebas de concepto para comparar soluciones en escenarios reales.
- **Estándares abiertos:** Priorizar soluciones que soporten estándares de la industria (como SIA OSDP, ONVIF) para garantizar interoperabilidad.
- **Evaluación de proveedores:** Confirmar capacidades de integración y probar interoperabilidad antes de comprar.
- **Escalabilidad:** Elegir tecnologías modulares o basadas en la nube que crezcan con las necesidades del negocio.
- **Enfoque en seguridad:** Evaluar cifrado, autenticación y certificaciones de cumplimiento.
- **Mantenimiento regular:** Programar revisiones, actualizaciones y evaluaciones de cumplimiento.
- **Capacitación:** Asegurar que el personal esté capacitado tanto en el uso de la tecnología como en mejores prácticas de seguridad.

CONCLUSIÓN

La Tecnología de Seguridad Operacional es fundamental para las misiones de seguridad modernas, pero su implementación exitosa requiere más que simplemente adquirir nuevas herramientas. La planeación estratégica, la colaboración entre stakeholders y la gestión continua del ciclo de vida son esenciales para lograr resultados críticos para la misión.

El informe OST de SIA es un recurso clave para navegar la complejidad del panorama actual de la tecnología de seguridad y garantizar operaciones de seguridad resilientes, escalables y efectivas.

DESCARGAR EL REPORTE COMPLETO DE SIA

SIA
SECURITY INDUSTRY ASSOCIATION