TECNOLOGÍA DE **SEGURIDAD** OPERACIONAL

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

SIA
SECURITY INDUSTRY ASSOCIATION

ALLEGION™ M.C. DEAN BUILDING INTELLIGENCE ONVIF® wesco

Acerca de los autores

John Deskurakis actualmente lidera la seguridad en Daikin Applied Americas, como Director de Seguridad de la Información (CISO) y Director de Información Adjunto (CIO adjunto). Su misión es transformar todos los elementos de seguridad en un modelo integrado y sin fricciones que pueda acelerar las capacidades empresariales y garantizar la resiliencia. Deskurakis fue director de seguridad de varios conglomerados mundiales de fabricantes de tecnología, como Carrier y Johnson Controls, donde apoyó directamente a una amplia gama de empresas y subsidiarias multinacionales, como LenelS2, Edwards, Kidde, Tyco, Software House, Exacq, Illustra, American Dynamics, Simplex, Grinnell y otras más. Previamente, dirigió esfuerzos de investigación y desarrollo seguros que impulsaron una variedad de complejos programas de defensa en Raytheon. Deskurakis también se desempeñó como Socio Gerente en CybrDesk, proveedores y consultores de tecnología de seguridad. Es experto en una variedad de temas de seguridad, con un importante enfoque en TI, tecnología operativa y tecnologías de seguridad.

Con múltiples títulos académicos, incluida una Maestría en Ciencias en Ciberseguridad de la Escuela de Ingeniería Whiting de la Universidad Johns Hopkins, una Licenciatura en Ciencias en Informática y una Licenciatura en Ciencias en Sistemas de Información de la Universidad del Sur de Florida, participa activamente en su comunidad, la academia y varias organizaciones comerciales. Deskurakis se ha desempeñado como presidente de la junta directiva del Consejo Asesor de Ciberseguridad de la Asociación de la Industria de Seguridad, miembro de la junta directiva de la Alianza Global de Ciberseguridad de la Sociedad Internacional de Automatización (ISA), miembro de la junta directiva del Instituto de Cumplimiento de Seguridad de ISA, miembro de la junta directiva del Consorcio de Ciberseguridad Inmobiliaria y panelista técnico de la Norma UL-2900-1 para ciberseguridad de software para productos conectables a redes.

Chris Lynch es ingeniero de software y arquitecto de seguridad, especializado en integración de sistemas y diseño de estrategias de seguridad en tecnologías operativas y sistemas de control industrial. Actualmente, está enfocado en la aplicación de estrategias proactivas para diseñar y entregar tecnologías operativas complejas dentro de la fabricación industrial. Lynch, con una licenciatura en ciberseguridad de la Universidad del Sur de Florida, es un ávido pescador, desarrollador de sistemas, investigador de seguridad, entusiasta de la tecnología y colaborador de publicaciones tecnológicas.

Índice

Apéndices y referencias

PRODUCIDO CON EL GENEROSO APOYO DE

SIA extiende su agradecimiento al liderazgo y a los empleados de Allegion, M.C. Agradecemos a Dean, ONVIF y Wesco por su apoyo en este informe y por su servicio y orientación como parte del comité directivo de este informe.

Resumen

No resulta controvertido sugerir que la mayoría de las empresas dependen considerablemente de la tecnología para funcionar al mínimo. Recurrimos a métodos tecnológicos para sentar las bases y mejorar nuestra prestación de servicios. Las capacidades que brindan estos medios pueden crear una ventaja o ayudar a lograr ventajas competitivas. Y si bien la dependencia de la mecanización y la automatización se ha convertido en un enfoque común para mejorar la eficacia, lograr consistencia, ofrecer valor y escalar la eficiencia operativa, los resultados tienden a variar notablemente. Cuando se trata de seleccionar, integrar, implementar y madurar las tecnologías destinadas a operacionalizar y mantener nuestras funciones comerciales principales, la mayoría de las organizaciones son fundamentalmente desiguales.

En la industria de la seguridad, lograr la excelencia dentro de nuestra pila técnica operativa es un objetivo importante para ayudar a garantizar el éxito de la misión. Tendemos a implementar y depender de algunos sistemas únicos para realizar las tareas de seguridad. Cuando se trata de nuestro software y hardware de seguridad, pueden existir desafíos importantes que suelen malinterpretarse u obviarse. Estas herramientas pueden ayudarnos a tener éxito, pero también pueden llevarnos al fracaso. Una comprensión más profunda de estas tecnologías nos brinda un mayor conocimiento de la situación y mitiga la probabilidad de errores y brechas comunes.

En un espacio operativo cada vez más complejo donde las amenazas evolucionan continuamente, es fácil entusiasmarse con la promesa de tecnologías de seguridad avanzadas y emergentes. Pero ese tipo de entusiasmo debe ser moderado por la realidad de que hay más oportunidades para errores, pasos en falso y disfunciones que para avances simples y fáciles de implementar. Una comprensión clara de los principios, desafíos y soluciones especialmente diseñadas garantizará el logro de resultados críticos para la misión y, al mismo tiempo, utilizará las tecnologías de seguridad operativa para defender y brindar una continuidad perfecta para tu negocio.

En este documento, exploraremos algunos de los tipos más destacados de tecnología de seguridad operativa (OST) y sus correspondientes desafíos, y analizaremos estrategias para garantizar una entrega óptima y las mejores prácticas operativas. El debate y los temas tratados son los más relevantes para los profesionales de la industria de la seguridad, así como la para tecnología de consumo de la industria de la seguridad en empresas pequeñas y medianas.

Relevancia

La demanda del mercado global de tecnología operativa (TO) ha evolucionado de manera sustancial en los últimos años. Con una tasa de crecimiento anual compuesta (CAGR) proyectada del 10% entre 2024 y 2030, se espera que esta tendencia del mercado continúe durante los próximos años.[1] Algunos de los factores clave que impulsan este dinámica son predecibles, pero vale la pena señalarlos. Mientras las empresas valoran las mejoras de eficiencia e intentan reducir los costos operativos, la complejidad de los sistemas, las demandas de los clientes y los requisitos competitivos están evolucionando.[2] Estas realidades, junto con la rápida adopción de tecnologías nuevas y emergentes como la inteligencia artificial (IA) y el aprendizaje automático, están impulsando una ola de modernización. [2] Si bien las versiones locales de los sistemas de TO tienden a ser las más comunes, la demanda de soluciones alternativas basadas en la nube está creciendo significativamente porque pueden reducir las barreras físicas y brindar mayor flexibilidad y escalabilidad. [1] Uno de los segmentos verticales más grandes del mercado de TO es el espacio de los sistemas de gestión de edificios (BMS), y esto es relevante para la industria de la seguridad. Se proyecta que durante los próximos cinco años, el crecimiento del mercado de TO dentro del segmento BMS será el de más rápido crecimiento, con una CAGR del 15,2%.[1]

Los profesionales de la industria de la seguridad están acostumbrados a la noción de tener que proteger lugares, personas y recursos importantes, como ciertos tipos de TO. Y en este sentido, existe una noción general dentro de la industria cuando imaginamos una variedad de tipos de TO, especialmente aquellos considerados parte de la infraestructura crítica. Los componentes de la TO también pueden ser un foco vital de muchos planes de seguridad y a veces incluso se piensa que son las joyas de la corona de una empresa.

La convergencia de la TO y la tecnología de la información (TI) ha sido un tema muy discutido en los últimos años. Pero lo que a veces se pasa por alto es la relación de ambos con la seguridad física. Una estrategia de seguridad integral depende en gran medida de la colaboración de diversas partes interesadas y de la alineación e integración técnica en ciertos dominios clave.[3] Las capacidades de TI, TO y seguridad (física y cibernética), por ejemplo, deberían crear sinergias. Sin embargo, en la práctica, aunque el acceso físico a muchas de las tecnologías que conectan dispositivos dentro de un entorno empresarial típico suele estar dentro del ámbito de la seguridad física, los tres dominios rara vez se entienden entre sí.[3]

Hay otra perspectiva. Los resultados y productos proporcionados por muchos elementos de la TO son bastante importantes para los objetivos diarios del personal de seguridad. Si bien puede no parecer obvio, el ecosistema de la TO promedio puede afectar significativamente las considerables responsabilidades de la misión de seguridad. No sólo nuestras herramientas y tecnologías de seguridad del sector están conectadas y dependen de dispositivos TO, sino que algunos de los programas y hardware de seguridad que utilizamos a diario pueden considerarse tecnología operativa por derecho propio. De hecho, la TO es una medalla con dos caras en cuanto a la seguridad. Comprender algunos de los principios y desafíos relacionados con los tipos de TO de los que dependemos a diario como profesionales de la seguridad puede marcar una diferencia significativa cuando nos enfrentamos a una complejidad creciente y a amenazas en evolución. Junto con las expectativas de cero fallos y al mismo tiempo garantizando resultados críticos para la misión, la TO es significativamente importante para la industria de la seguridad.

1 Tendencias del mercado de la tecnología operativa. Visto el: 26 de octubre de 2024. [Online]. Disponible en inglés: https://www.grandviewresearch.com/industry-analysis/operational-technology-market-report (Grand View Research, 2024)
2 Tamaño y pronóstico del mercado de la tecnología operativa. Visto el: 26 de octubre de 2024. [Online]. Disponible en inglés: https://www.verifiedmarketresearch.com/product/operational-technology-market (Verified Market Research, 2024)
3 7 pasos para alinear TI, TO y seguridad física. Visto el: 26 de octubre de 2024. [Online]. Disponible en inglésinglés: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/11/29/7-steps-to-align-it-ot-and-physical-security. (IANS 2022)

Simplificación

Para empezar a entender algo, debemos empezar por especificar de qué estamos hablando. Definir qué es, qué hace y qué no es la tecnología operativa puede ser un desafío. A menudo se convertirá en fuente de encendidos debates, especialmente entre operadores técnicos de diferentes industrias, disciplinas y dominios. Es importante, como mínimo, acordar algunos de los conceptos y definiciones fundamentales antes de sumergirse en cualquier discusión técnica. ¿Pero cómo llegamos allí?

Si consideramos cuidadosamente la causa fundamental de este tipo de amables desacuerdos, rápidamente nos daremos cuenta de que la TO tiende a existir en puntos de convergencia y a menudo se intersectará con una variedad de necesidades, requisitos y funciones utilitarias. Y en estas intersecciones, el contexto, el propósito y los detalles a menudo variarán. Por lo tanto, la interpretación humana estará influenciada por una diversidad de experiencias separadas y puntos de vista resultantes. Las definiciones naturalmente se volverán divergentes.

Esta es una consideración importante porque, si bien escuchamos con frecuencia el término "tecnología operativa" y sabemos que juega un papel importante en nuestra vida diaria, a menudo no reconocemos nuestra forma individualizada de pensar al respecto. Esta falta común de autoconciencia del pensamiento puede ser el origen de la fricción que experimentamos cuando nos damos cuenta de que no estamos alineados con nuestros colegas en los conceptos y definiciones básicos dentro de las discusiones de la TO y otros temas similares. ¿Cómo podemos entonces crear sinergias en nuestras bases para que podamos centrarnos en la exploración e identificación de los desafíos y oportunidades que nos llevarán a mayores resultados? En términos simples, estamos de acuerdo sobre el alcance y ajustamos específicamente una definición para que podamos llevar a debates saludables por consiguiente.

Si comenzamos buscando definiciones generales de TO, descubriremos que a menudo se piensa en ella como algo puramente industrial en un contexto. Por ejemplo, Cisco dice que "la TO sirve para conectar, monitorear, administrar y proteger las operaciones industriales de una organización. Las empresas que se dedican a actividades como manufactura, minería, petróleo y gas, servicios públicos y transporte, entre muchas otras, dependen en gran medida de la TO."[4] Si bien eso es cierto, hay otros puntos de vista y otras definiciones "verdaderas".

Algunos dirán que la TO es específicamente hardware. Pero otros lo rebatirán. Por ejemplo, Gartner sugiere que la TO es "hardware y software que detecta o provoca un cambio, a través del monitoreo y/o control directo de equipos, activos, procesos y eventos industriales."[5] Esto también parece cierto, pero es una interpretación más amplia y es posible que no coincida exactamente con la de Cisco. Por otra parte, quizás sí. Define "equipo industrial". Todo depende de la perspectiva, por supuesto.

RedHat afirma que mientras que "los sistemas de TO se utilizan principalmente para interactuar con el mundo físico, los sistemas TI se utilizan principalmente para resolver problemas comerciales de los usuarios finales."[6] Aunque se podría decir que la primera parte de la oración captura la esencia de lo que prácticamente cualquier TO hace, la segunda parte probablemente pueda ser debatida si se le da un contexto adicional. Por ejemplo, los sistemas de control industrial, como los controladores lógicos programables, también resuelven problemas comerciales, permiten la automatización y brindan valor a los usuarios finales. También resultan ser capaces de interactuar con el mundo físico. Son controladores industriales. Esta definición puede ser confusa y requeriría una definición indiscutible de

4 ¿En qué se diferencian la TO y la TI? Visto el: 27 de octubre de 2024. [Online]. Disponible en inglés: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html (Cisco)
5 Tecnología operativa (TO) Visto el: 27 de octubre de 2024. [Online]. Disponible en inglés: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot (Gartner)
6 ¿Qué es la tecnología operacional? Visto el: 27 de octubre de 2024. [Online]. Disponible en inglés: https://www.redhat.com/en/topics/edge-computing/what-is-ot (Red Hat, 2022)

"problema empresarial." Lo que está claro es que las opiniones varían. Y si bien algunos argumentarían que las tres significan lo mismo, otros no estarían de acuerdo. Todos los puntos de vista aportan valor cuando empezamos a centrarnos en los planteamientos de los problemas y las soluciones relacionadas con la TO.

Aunque definir la TO puede resultar subjetivo, condicional e incluso depender del contexto, las condiciones que impulsan la comprensión relativa suelen estar relacionadas con nuestra propia industria, prácticas, necesidades y/o uso previsto. Los diversos puntos de vista que a veces generan definiciones divergentes también pueden unirse para formar una base sólida de comprensión y una visión generalizada de la TO. Después de una cuidadosa reflexión, podemos ver que la mayoría de las definiciones aparentemente contradictorias son todas correctas, en el contexto adecuado. Por lo tanto, las opiniones divergentes deberían considerarse como aportes valiosos para una mayor comprensión.

Para los propósitos de esta discusión, no es necesario definir lo que significa la TO para cada persona, cada situación y cada aplicación. El abanico completo de temas relacionados con la TO sería demasiado amplio y en gran medida no relacionado con nuestra respectiva misión de seguridad. Lo esencial es limitar el alcance para que podamos desarrollar cierta especificidad dentro de nuestro espacio problemático.

Por lo tanto, deberíamos comenzar por recordar que operamos dentro de un sector horizontal específico: el de la seguridad. Considerando nuestro enfoque y responsabilidades únicos, sería prudente limitar el alcance de nuestra discusión con base en cómo la TO se relaciona con nosotros. Además, en lugar de pensar en la TO en el contexto de lo que podríamos proteger, deberíamos aplicar un poco de pragmatismo en nuestro temperamento concentrándonos en las tecnologías que nos ayudan a operar como profesionales de la seguridad. ¿Cuál es nuestra versión de la TO? ¿Hay seguridad en la TO? Al refinar el campo de esta manera podemos garantizar mejor la precisión, la relacionabilidad y lograr una conversación sólida. Además, ¡es práctico!

Con esto en mente, desarrollaremos una definición de tecnología de seguridad operativa (TSO). Considéralo un subconjunto de la TO, con muchas de las mismas cualidades para garantizar un éxito operativo relativo dentro de nuestro campo distintivo. Definiremos la TSO como los elementos técnicos subyacentes que nos permiten realizar nuestro trabajo como profesionales de la seguridad. No es necesariamente maquinaria industrial, pero puede serlo. Las TSO son las tecnologías que nos ayudan a escalar, automatizar y garantizar resultados de seguridad exitosos. Todos sirven para respaldar y cumplir la misión principal de la seguridad física. Las TSO son, por lo tanto, tecnologías que, de alguna manera, nos conectan con el mundo físico que intentamos proteger y ayudan a gestionar los problemas de seguridad.

Recordemos nuestra discusión sobre la subjetividad. Dentro de nuestro limitado alcance, podríamos ajustar ligeramente algunas de las definiciones prevalecientes de TO revisadas anteriormente, con un toque de seguridad. Imaginamos que Cisco podría decir ahora: "La TSO sirve para conectar, supervisar, gestionar y entregar las operaciones de seguridad de una organización." Quizás Gartner diría que "la TSO es hardware y software que detecta o provoca un cambio a través del monitoreo y/o control directo de equipos, activos, procesos y eventos de seguridad." RedHat podría afirmar que "los sistemas de TSO se utilizan principalmente para interactuar con el perímetro de seguridad y para resolver problemas de seguridad de los usuarios finales."

Resulta interesante notar que cuando limitamos nuestro alcance e infundimos algún contexto específico del dominio, de repente los puntos de vista que suenan algo diferentes y las diversas definiciones comienzan a converger y alinearse. Aplicando nuestras propias condiciones específicas de la industria, seguimos adelante.

Magnificación

No hay que subestimar la complejidad real de nuestro alcance refinado. Existen muchos tipos de TSO que pueden conectarse, integrarse y automatizarse de diferentes maneras dentro del mundo de la seguridad. Dependemos de estos sistemas para ayudar a garantizar requisitos específicos de seguridad física y operativa. Se utilizan para resolver problemas importantes empresariales y de usuario final. Contamos con la TSO para lograr resultados críticos para la misión. Tecnologías como los sistemas de control de acceso físico (PACS), sistemas de vigilancia, dispositivos de detección, controles perimetrales y ambientales y soluciones de gestión de seguridad, entre otros, pueden ayudar a garantizar que nuestras tareas como profesionales de la seguridad sean más fáciles de respaldar y se realicen de manera consistente y exhaustiva.

Sin embargo, a pesar de los muchos problemas que la TSO puede gestionar, mitigar y resolver, también pueden estar repletas de complejidad y trampas que pueden generar distracciones y ruido blanco, e incluso disminuir el valor que se pretende brindar. Las soluciones de TSO complejas pueden brindar muchos beneficios, pero no siempre son fáciles de implementar y mantener. La implementación, la integración y el mantenimiento continuo del ciclo de vida no son tan simples en muchos casos y deben planificarse y manejarse con cuidado. Sin proactividad, una comprensión profunda de los enunciados de los problemas, experiencia en el dominio y una estrategia sistémica, la síntesis y coordinación de la TSO pueden convertirse en el foco de atención a tiempo completo, suplantando nuestro "trabajo diario" habitual dentro de las operaciones de seguridad. Las interrupciones por sí solas pueden llegar a ser perjudiciales para la misión principal y afectar la postura de seguridad que la TSO busca mejorar.

Peor aún, muchas fallas relacionadas con la tecnología suelen surgir cuando elegimos una TSO que no se ajusta a nuestras necesidades específicas. Los requisitos pueden ser ilusorios. La selección de una

tecnología puede ser imprecisa y costosa cuando se toman decisiones imprudentes. Aun si hemos planificado bien y tomado decisiones inteligentes al seleccionar una TSO, simples defectos de integración pueden causar brechas de seguridad y fallas de sincronización entre elementos de seguridad físicos y digitales. Estos errores pueden generar vulnerabilidades y resultados inconsistentes. Cuando se combinan múltiples tecnologías complejas diseñadas por diferentes fabricantes de equipos originales (OEMs) para crear capacidades integradas dentro de una pila de seguridad en malla, las partes interesadas tienden a esperar ciegamente que el nuevo sistema unificado funcione inherentemente bien. Damos por sentado que conectará a los usuarios con más información y garantizará mejores resultados. Pero la realidad suele ser diferente. En una encuesta reciente, casi la mitad de los administradores de PACS informaron que mejorar la comodidad del usuario es difícil, mientras que aproximadamente una cuarta parte de los encuestados afirmó que uno de sus tres principales desafíos era integrar sus sistemas de seguridad con otros sistemas empresariales.[7] Esto es relacional.

La TSO debe operar dentro de un ecosistema más amplio de tecnologías que no son necesariamente parte de la misión de seguridad. La mayoría de los elementos, TSO o no, normalmente no están pensados para funcionar juntos y ni siquiera están diseñados comúnmente en la misma época. Las modernas tecnologías se conectan regularmente a componentes heredados con una serie incongruente de capacidades de rendimiento, requisitos de recursos y limitaciones divergentes. Cuando comenzamos a conectar estos sistemas disímiles, a menudo se da por sentado que se obtendrán resultados consistentes y una interoperabilidad limpia, pero rara vez esto es realista si no se cuenta con un considerable conocimiento del dominio técnico, planificación y esfuerzo. A veces, uno o más subsistemas simplemente no funcionan con el resto. Por desgracia, asumir el peor resultado de la interoperabilidad es la presunción más prudente.

Cuando consideramos la integración, también debemos tener en cuenta la interoperabilidad. Conectar sistemas entre sí ya es bastante complicado, pero ahora debemos pensar un nivel más profundo y contemplar la posibilidad de que estos sistemas intercambien información y luego hagan algo valioso con esos datos. También debemos garantizar que sistemas separados en el mismo entorno puedan funcionar según lo diseñado en concurrencia sin impactar a los demás. No hay una clara comprensión de lo que ocurrirá en las etapas anteriores y posteriores del proceso. Los problemas de interoperabilidad y la incompatibilidad entre sistemas diseñados para funcionar como un súper sistema unificado pueden generar ineficiencias, brechas de seguridad y menor supervisión. Esto puede costar a las partes interesadas una gran pérdida de tiempo y dinero.

Consideremos los posibles impactos directos de las fallas de interoperabilidad en la misión de seguridad. Si tus diferentes sistemas no se integran fácilmente, también puede valer la pena explorar si una plataforma de gestión de instalaciones inteligentes podría reducir las barreras de interoperabilidad y proporcionar una postura de seguridad más sólida. La reducción de la automatización y la mecanización generalmente dará como resultado un aumento de las actividades manuales y una mayor carga de trabajo humana.[8] Los operadores de seguridad sobrecargados son más propensos a cometer errores o a no identificar brechas de seguridad.[9] Los sistemas dispares tienden a caracterizarse por silos de datos, lo que puede causar demoras, malentendidos, tiempos de respuesta reducidos o imposibilidad de identificar amenazas.[10]

Consideremos por un momento la integración del sistema de video. Según Leo Levit, presidente del Foro de Interfaz de Video en Red Abierta (ONVIF), "si los sistemas se conectan pero no pueden compartir y usar los datos adecuadamente, esto genera problemas como ineficiencias o riesgos de seguridad. Los protocolos ONVIF permiten que distintos componentes trabajen juntos de manera más fluida, evitando problemas de datos que causan demoras y amenazas no detectadas. El costo de una falla en la interoperabilidad no es sólo financiero: cuando la automatización falla, afecta directamente a los operadores humanos, quienes se ven sobrecargados por los procesos manuales. El compromiso de ONVIF con la estandarización aborda tanto los aspectos técnicos como operativos de este desafío."

Hay que tener en cuenta muchos otros desafíos antes de introducir nuevas soluciones de TSO, como las limitaciones operativas, la facilidad de uso, los requisitos reglamentarios y las demandas logísticas, así como las preocupaciones de eficiencia y escalabilidad. Existen requisitos de usuario, modelos de negocio y obligaciones de entrega que pueden no alinearse bien con las soluciones técnicas que se entregan en nuestro entorno. Para complicar aún más las cosas, es posible que tu OEM de tecnología esté en proceso de modernizar los sistemas que utilizas de una manera que podría resultar perjudicial para tu entorno.

Tal vez, por ejemplo, el OEM de tu solución PACS esté transformando el software alojado localmente, que conoces y te gusta, en una nueva oferta SaaS basada en la nube. Puede sonar maravilloso, más moderno, universalmente accesible y escalable, pero también puede ser incongruente con tu entorno y las realidades de las capacidades de soporte locales. Puede que el nuevo avance resulte difícil o incluso imposible de gestionar para el personal actual. Si trabajas con un distribuidor o integrador de tecnología, no des por sentado que se encargarán del mantenimiento de

tus instancias de nube que requiere la oferta. Ten en cuenta que los requisitos funcionales y del sistema no siempre son lo suficientemente claros.

A veces, las tecnologías emergentes no se alinean adecuadamente con el resto de tu pila de seguridad y el ecosistema tecnológico de tu edificio, donde se ubica tu TSO. Las nuevas innovaciones pueden presentar nuevos riesgos y dificultades que todavía no estamos preparados para gestionar o de los que no somos conscientes. Es fundamental comprender todos los aspectos de la TSO de la que dependerás. Desde la selección hasta la integración, la implementación, el mantenimiento, las actualizaciones, las transferencias y el soporte del ciclo de vida, todas las facetas deben coincidir con tus propias necesidades y capacidades.

Muchas cosas pueden salir mal. Comienza con una estrategia que incluya una consideración prudente de los aspectos esenciales y los resultados del negocio. Planifica la evaluación, análisis y pruebas continuas. Si bien algunos de los desafíos centrales más obvios y complicados relacionados con la TSO se pueden encontrar en los detalles y dentro del ámbito de la integración, la interoperabilidad y el rendimiento, existen otros obstáculos que pueden no ser tan predecibles. Las asociaciones estratégicas con proveedores y una experiencia confiable en el dominio son imprescindibles.

7 Control de acceso físico: Encuesta revela nuevas tendencias de implementación, L. Merredew. Visto el: 2 de noviembre de 2024. [Online]. Disponible en inglés: https://www.securitymagazine.com/articles/98710-physical-access-control-survey-reveals-new-deployment-trends. (Security Magazine, 2022)

8 Cómo la automatización obsoleta conduce a un mayor esfuerzo manual y qué puedes hacer al respecto, N. Kinson. Visto el: 3 de noviembre de 2024. [Online]. Disponible en inglés: https://www.redwood.com/article/how-outdated-automation-leads-to-more-manual-effort-and-what-you-can-do-about-it (Redwood, 2022)

9 Por qué los empleados con exceso de trabajo son un riesgo para la seguridad, D. Kelley. Visto el: 3 de noviembre de 2024. [Online]. Disponible en inglés: https://securityintelligence.com/security-risk-staffing-it-teams-overworked-employees (Security Intelligence, 2014)

10 Interoperabilidad de sistemas de seguridad y protección, Pkimluker. Visto el: 9 de noviembre de 2024. [Online]. Disponible en inglés: https://www.clr2wrk.com/safety-and-security-systems-interoperability (Clear 2 Work, 2022)

Identificación

Dejando de lado por un momento el panorama más amplio de las realidades del ecosistema y los desafíos operativos, pasamos a la parte T de la TSO como nuestro próximo paso. Nos enfocaremos ahora en los elementos tecnológicos que posibilitan las operaciones en el mundo de la seguridad. A pesar del alcance limitado de nuestra discusión, hay que considerar una amplia gama de tipos de componentes, sistemas y subsistemas cuando pensamos en la TSO. Si nos limitamos sólo a los elementos básicos que deben conectarse y funcionar bien dentro de un ecosistema de seguridad unificado, como PACS, BMS, componentes de vigilancia y monitoreo, sensores, alarmas, equipos contra incendios y seguridad, herramientas cibernéticas, sistemas de TI y sistemas basados en la nube, podemos darnos cuenta que dominar todo no es una perspectiva sencilla. Estos elementos variados de la TSO no son simples y suelen requerir un soporte diferenciado. Los componentes del sistema de seguridad por lo general no son tecnologías elementales del tipo "plug and play". No siempre son compatibles entre sí. A menudo se requiere y siempre se recomienda apoyo profesional.

Para conceptualizar mejor la escala y el alcance del espacio de la TSO, es útil desarrollar una amplia visión que describa algunos de los tipos clave de tecnologías. Si bien esta no es una compilación completa de todas las TSO, proporciona una comprensión de la amplia gama de diferentes elementos del sistema que uno probablemente encontrará dentro de la pila de seguridad común. Hay mucho en qué pensar cuando empezamos a profundizar en la TSO. A continuación definiremos y aclararemos los principales tipos de categorías que se presentan. A medida que profundizamos en algunos de los elementos componentes dentro de las cinco columnas de la Tabla 1 (Tecnología de seguridad operativa común), nuestro objetivo es desarrollar una mejor comprensión general de los desafíos para iluminar las mejores prácticas, la estrategia y la planificación.

Tabla 1 – Tecnología de seguridad operacional común (TSO), por categoría

Sistemas de control de acceso físico (PACS)	Sistemas de vigilancia	Sistemas de detección (alarmas y sensores)	Seguridad perimetral y ambiental	Gestión de la seguridad
Sistemas de tarjetas de acceso	Circuito cerrado de televisión	Detección de patrones anómalos	Gestión de edificios Sistemas (BMS)	Centro de operaciones de seguridad física
Sistemas biométricos	Cámaras IR	Alarmas inteligentes	Sistemas de respaldo de energía y comunicaciones	Monitoreo remoto
Acceso con código PIN	Cámaras con movimiento horizontal, vertical y zoom	Radar y LiDAR	Barreras y bolardos	Tecnología de análisis de video
Gestión de identidad y acceso (IAM)	Cámaras termográficas	Tecnología de geocercas	Soluciones de cercas	Sistemas de notificación de incidentes
Autenticación de múltiples factores (MFA)	Cámaras corporales	Sensores sísmicos	Alambre de púas y de cuchillas	Sistemas de notificación masiva
Puertas entrelazadas	Tecnología de reconocimiento de patrones	Dispositivos de pánico	Tecnologías de puertas	Sistemas de torres de vigilancia
Sistemas de torniquetes	Cámaras de reconocimiento facial	Detectores de humo y gas	Control de acceso de vehículos	Dispositivos de comunicación
Cerraduras inteligentes	Cámaras activadas por movimiento	Detectores de agua, temperatura, calor y humedad	Torniquetes	Sistemas PA
Sistemas de control de acceso móviles	Sistemas de reconocimiento de placas vehiculares	Sensores de movimiento, vibración y manipulación	Trampas y vestíbulos de seguridad	Sistemas de detección y extinción de incendios
Puertas de seguridad	Sistemas de monitoreo remoto de video	Monitoreo acústico	Cabinas de seguridad	Sistemas de salida de emergencia
Sistemas de gestión de visitantes	Sistemas de vigilancia y almacenamiento en la nube	Sistemas de detección de drones	Iluminación, señalización y elementos disuasorios físicos	Plataformas de seguridad integradas
Etiquetas RFID	Analíticas de video	Sensores magnéticos	Contraventanas y ventanas resistentes	Dispositivos de seguridad del Internet de las Cosas (IoT)
Gestión de credenciales SW	Grabadores de video en red	Sensores de presión y rotura de cristales	Barreras de drenaje y contra inundaciones	Capacidades de ciberseguridad
Sistemas de reconocimiento de identidad	Drones y robots	Detectores de campo de microondas	Sistemas de contención	Rastreo GPS

Sistemas de control de acceso físico (PACS)

Cuando se habla de TSO es casi inevitable empezar la conversación refiriéndonos a los PACS. Esto porque, después de todo, es la primera línea de la mayoría de las defensas físicas organizacionales. Estos sistemas generalmente sirven como puerta de entrada protectora, defendiendo activos valiosos y brindando acceso autorizado. Garantizan que sólo las partes autorizadas tengan acceso a recursos críticos. Para aclarar, un PACS es un sistema electrónico o digital que otorga acceso físico a personas autorizadas mediante la confirmación de identidades, utilizando tarjetas clave, credenciales móviles, biometría y otros factores de autenticación.[11] La Tabla 2 proporciona una excelente descripción general de algunos de los componentes principales que se encuentran dentro de la implementación común de los PACS.

Si bien los sistemas de control de acceso basados en tarjetas tienden a ser uno de los tipos más comunes de soluciones PACS que las organizaciones utilizan hoy en día, las estrategias de seguridad modernas están evolucionando y la complejidad está creciendo.[12] Por ejemplo, en muchas operaciones las estrategias de seguridad física y ciberseguridad están convergiendo, lo que da como resultado que los PACS se integren cada vez más regularmente con los sistemas de control de acceso lógico (LACS).[13] Los LACS por lo general se utilizan para gestionar y estandarizar el acceso de los usuarios a redes informáticas, sistemas y datos. Y hay una motivación utilitaria para ello. En pocas palabras, gran parte de los datos disponibles en cualquiera de los sistemas son útiles para ambos. Entonces ¿por qué no compartirlos?

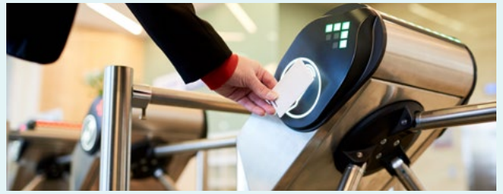
Tabla 2 – Componentes comunes de PACS

Componente	Descripción
Punto de acceso	Punto de ingreso o barrera física donde un individuo interactúa con el PACS. Por ejemplo, los puntos de acceso incluyen torniquetes, portones y puertas con cerradura.
Lector de credenciales y teclado	El lector proporciona energía y lee datos de una credencial física. También envía estos datos a un panel de control para autenticar la credencial y solicitar autorización de acceso. Dependiendo de las políticas específicas de la instalación, es posible que las personas necesiten introducir un PIN en el teclado o un dato biométrico.
Lector biométrico	Captura datos biométricos (como la huella dactilar, la imagen facial o el escaneo del iris) y los verifica con los datos biométricos de credenciales conocidos o almacenados.
Panel de control	Recibe los datos de credenciales que envía el lector y verifica su presencia en el repositorio de datos del titular de la credencial. Luego toma una decisión de acceso y transmite datos de autorización al servidor de control de acceso y al punto de acceso.
Servidor de control de acceso	Otorga autorización a personas que solicitan acceso (por ejemplo, presentando una credencial de tarjeta de acceso a un lector). También registra e inscribe individuos, inscribe y valida credenciales y registra eventos del sistema.
Repositorio de datos de titulares de credenciales	Contiene datos de identidad individual y privilegios de acceso físico. Los paneles de control utilizan estos datos autorizados para validar los datos de credenciales.
Sistemas auxiliares	Las organizaciones pueden integrar el PACS con sistemas de monitoreo de instalaciones adicionales, como sistemas de vigilancia, alarmas contra incendios y sistemas de evacuación.

Fuente: http://www.idmanagement.gov/university/pacs

11 Fundamentos de los sistemas de control de acceso físico Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://www.idmanagement.gov/university/pacs/ (Oidmanagement.gov, 2023)
12 10 tipos de sistemas de control de acceso físico, OLOID Desk. Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://www.oloid.ai/blog/10-types-of-physical-access-control-system (Oloid, 2023)
13 Integración de IAM con sistemas de control de acceso físico, D. Simmons. Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://techvisionresearch.com/wp-content/uploads/2020/03/PACS-LACS-20200310-excerpt-final.pd (TechVision Research, 2020)

Los LACS tienden a asociarse más comúnmente con implementaciones de gestión de acceso e identidad (IAM) centradas en TI. Pero en un mundo convergente, se integrarán más sistemas a través de líneas cada vez más difusas de silos tecnológicos. Gartner señala que, "los líderes de seguridad y gestión de identidades y accesos (IAM, por sus siglas en inglés) asumirán un rol creciente en la selección, implementación y operación de nuevas tecnologías de control de acceso físico (PACS)."[14] Esto se debe a que la convergencia entre TI, TO y las operaciones genera una mayor eficiencia.



Sistemas de control de acceso físico

- Sistemas de tarjetas de acceso
- Sistemas biométricos
- Acceso con código PIN
- Gestión de identidad y acceso
- Autenticación de múltiples factores
- Puertas entrelazadas
- Sistemas de torniquetes
- Cerraduras inteligentes
- Sistemas de control de acceso móviles
- Puertas de seguridad
- Sistemas de gestión de visitantes
- Etiquetas RFID
- Gestión de credenciales SW
- Sistemas de reconocimiento de identidad

El mundo está cambiando. Pero, ¿qué pasa con las organizaciones que carecen de equipos de seguridad amplios y del conjunto de líderes funcionales que, según nos dice Gartner, ahora están empezando a trabajar juntos? Las pequeñas y medianas empresas (PYMES), por ejemplo, tienden a depender de recursos internos limitados, complementados con relaciones con socios proveedores para garantizar que la misión de seguridad esté bien respaldada. En estos casos, la complejidad puede incluso aumentar. Los enfoques estándar diseñados para grandes corporaciones no son suficientes para las PYMES. Aquí es donde se vuelven cruciales una comprensión profunda de las propias necesidades y requisitos únicos, y las alianzas adecuadas.

Para el responsable de una PYME, a continuación describiremos un experimento mental de punto de partida (utilizando PACS como estudio de caso) para comenzar la exploración y ayudar a evitar errores comunes. Encontrar el camino correcto para el éxito individual varía.

1. **Los aspectos fundamentales.** Busca las soluciones y tecnologías que mejor se adapten a tus necesidades específicas. Las tecnologías emergentes y las soluciones de moda no siempre son adecuadas. Los requisitos simples se pueden gestionar de forma sencilla. Construye una base sólida de los conceptos básicos y perfecciona a partir de ella. Construye a la medida, según la prioridad de tus necesidades y tu modelo operativo. Sé capaz de responder a esta pregunta: "¿Qué problema(s) estoy tratando de resolver?" Luego identifica la solución.
2. **Un pronóstico gris.** Los OEMs están introduciendo cada vez más soluciones PACS basadas en la nube con la intención de comercializar ventajas de escalabilidad y presentar una alternativa de "hazlo tú mismo" para las PYMES. Si bien estas opciones pueden ser adecuadas para ti, hay preguntas a responder:
   a. **Costo –** Alojar tecnología en la nube no siempre es tan económico como parece. Claro que puede haber ahorros: Pero ¿existen gastos ocultos de funcionamiento, soporte y experiencia en el dominio? Determina el costo total de propiedad (TCO) con anticipación.
   b. **Experiencia** – La mayoría de las PYMES carecen del personal necesario para implementar, integrar y soportar sistemas alojados en la nube a perpetuidad. Nunca es tan simple como lo anuncian. Asegúrate de estar consciente de lo que se necesita para jugar en este espacio.
   c. **Cumplimiento normativo y seguridad** – La protección de los datos alojados no es algo garantizado y tu proveedor de nube sólo es responsable hasta cierto punto. Como propietario de la instancia, mantendrás muchas responsabilidades de seguridad de forma independiente. Garantizar el cumplimiento de las regulaciones específicas de la industria relacionadas con los datos será una capa adicional de complejidad requerida.
   d. **Rendimiento** – Mantener un alto rendimiento después de la migración a la nube no siempre es sencillo y sin complicaciones. Mucho dependerá de las limitaciones específicas de tu sistema, los requisitos de usuario y soporte, y las necesidades de tu negocio.
   e. **Bloqueo del proveedor** – Una vez que comienzas a depender de un proveedor de nube, puede resultar difícil o costoso migrar o realizar cambios sustanciales. Asegúrate de comprender cómo podría ser un plan de salida, por si acaso.
   f. **Preparado para el futuro** – Al implementar soluciones basadas en la nube, las PYMES deben garantizar consideraciones de escalabilidad y crecimiento. Por ejemplo, ¿puede la infraestructura de red soportar la probabilidad de un aumento de tráfico en el futuro?
3. **Si suena demasiado bueno para ser verdad...** Antes de asumir que una solución PACS es tan sencilla como "hazlo tú mismo", asegúrate de saber en qué te estás metiendo. Incluso si buscas ayuda de terceros, haz alguna tarea de forma independiente. Ten en cuenta muchos de los desafíos descritos en este documento, revisa los recursos proporcionados en los apéndices y siempre consulta con un socio proveedor o profesional de confianza.
4. **Preparación.** Ya sea que trabajes con un socio de integración confiable o intentes actualizar o introducir un nuevo PACS por tu cuenta, hay algunas acciones de planificación clave que debes considerar. Los siguientes consejos preliminares se basan en la orientación de idmanagement.gov y se han perfeccionado para nuestros propósitos y alcance de la discusión.[11]
   a. Identifica a tus partes interesadas desde el principio y designa un líder de proyecto PACS.
   b. Designa personal para cubrir roles clave cuando sea posible. Según sea necesario, recurre a socios de confianza para que actúen como arquitectos, ingenieros, integradores, evaluadores y operadores.
   c. Involucra a expertos en tecnología y dominio de seguridad desde el principio. Los CISOs y CIOs son tus amigos. Recurre a ellos.
   d. Solicita la creación, mantenimiento y disponibilidad de un cronograma maestro integrado durante la vida útil de tu proyecto. Este documento debe incluir las fases del proyecto, tareas, recursos y dependencias. Se deben designar partes responsables.
   e. Establece un plan de gestión del ciclo de vida de los PACS para ayudar a estimar las actualizaciones de hardware y software a lo largo del ciclo de vida operativo de los sistemas. Piensa en el Costo Total de Propiedad (TCO).
   f. Incluye el costo del licenciamiento del software y el mantenimiento del sistema en el presupuesto de tu proyecto. Identifica todos los costos de mantenimiento del sistema relacionados como un TCO anualizado.
   g. Trabaja con técnicos e ingenieros del sitio o de las instalaciones para identificar las limitaciones específicas de tu espacio objetivo. Estas restricciones pueden ser un factor limitante en la selección de tecnología.

14 Perspectiva tecnológica para sistemas de control de acceso físico. Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://www.gartner.com/en/documents/3451120 (Gartner, 2016)

h. Planifica estrategias de implementación estandarizadas específicas para cada sitio.

i. Recuerda que es posible que los elementos del sistema antiguo, como los lectores de credenciales, no soporten los nuevos modos de operación requeridos para los estándares de cumplimiento.

j. Utiliza credenciales antiguas y modos de operación no compatibles sólo en una estrategia de migración, no como estado final. Los planes finales de estado deben estandarizar el cumplimiento normativo.

k. Retira y elimina gradualmente las credenciales secundarias y antiguas.

l. Utiliza el sistema de gestión de identidad basado en LACS de tu organización como fuente autorizada para todos los registros de usuarios en el PACS, si es posible.

m. Algunos PACS permiten la asignación de niveles de acceso de usuarios al momento del registro de credenciales. Planifica el método de asignación antes del aprovisionamiento/registro.

n. Utiliza un enfoque basado en el riesgo al seleccionar mecanismos de autenticación apropiados para el acceso físico a edificios e instalaciones.

o. Recuerda que los puntos de acceso no deben depender únicamente de un mecanismo de autenticación que requiera funciones de tarjeta opcionales. Es posible que estas funciones no estén disponibles en todas las tarjetas de población de usuarios.

p. Diseña y configura PACS que respondan a las necesidades del entorno de destino. Por ejemplo, no requieras autenticación de múltiple factor (MFA) cuando sólo se necesite un factor.

q. La PKI es la base para implementaciones de PACS de alta seguridad. Planifícala.

r. Siempre hay más. Consulta con un profesional y busca continuamente la mejora.

5. **Operacionalización de la TSO**. El trabajo no termina después de haber planificado de manera proactiva la implementación de un nuevo sistema y de haberlo integrado e implementado con éxito. Poner en funcionamiento tu TSO para PACS es otra tarea que requiere mucha consideración. Los siguientes consejos preliminares se basan en la orientación de idmanagement.gov y se han perfeccionado para nuestros propósitos y alcance de discusión.[11]

   a. El éxito de la misión requiere personas, procesos y herramientas. Ahora que tienes las herramientas, asegúrate de contar con las personas adecuadas y los procesos diseñados específicamente para ese fin. Asegúrate de que tu enfoque se ajuste a las necesidades de tu negocio, que sea sólido y que mejore continuamente.

   b. Las cosas saldrán mal. Define procesos y procedimientos claros para resolver requisitos comerciales y de usuarios, así como errores e incidentes del sistema. Por ejemplo, podrían aparecer lectores de credenciales defectuosos. La tarjeta de acceso de un empleado puede perderse o quedar inoperable. Ten planes para resolver los problemas inevitables.

   c. Asegúrate de identificar al personal de soporte clave y los niveles de soporte esperados.

   d. Realiza un mantenimiento regular del sistema y la aplicación de parches a los componentes del PACS.

   e. Establece procedimientos claros para probar las actualizaciones antes de su implementación generalizada. Desarrolla procedimientos de reversión cada vez que se actualice o se pase a nuevas versiones.

   f. Asegúrate de que PACS esté configurado y mantenido para funcionar en estados compatibles. Revisa periódicamente los requisitos de cumplimiento, políticas y gobernanza.

   g. Trabaja con tus profesionales de TI y ciberseguridad para garantizar que PACS tenga parches, actualizaciones, sea seguro y funcione de manera eficiente periódicamente.

   h. Asegúrate de contar con un plan adecuado de gestión de identidad y acceso, que se mantenga y revise periódicamente. Asegúrate de que las identidades del sistema se gestionen de acuerdo con los estándares de la industria y los requisitos comerciales.

   i. Elimina toda la información de identificación personal de los puntos finales de PACS para proteger la privacidad.

   j. Realiza auditorías periódicas de la funcionalidad del sistema. Por ejemplo, verifica que los puntos de acceso estén utilizando la cantidad y el tipo correctos de factores de autenticación. Considera utilizar credenciales de prueba que hayan expirado o hayan sido revocadas para garantizar el correcto funcionamiento.

La conclusión fundamental es bastante simple: Aunque las soluciones PACS pueden parecer simples a primera vista, están lejos de serlo. ¿Dijimos que esto era sencillo? Los PACS se conectan a muchas cosas, desde la puerta de entrada de un edificio hasta ascensores y recursos críticos de la empresa. Poner estos sistemas en funcionamiento y listos puede ser una ardua tarea. Existe una serie de obstáculos menos obvios. Conocerlos bien ayudará a garantizar el éxito operativo.

La preparación y la orientación operacional proporcionadas en esta sección se pueden generalizar y adaptar a casi cualquier implementación de una TSO. La lección clave a entender es que cualquier implementación exitosa de una TSO requiere este nivel de pensamiento estratégico. Los PACS son un gran ejemplo para este ejercicio porque se encuentran de forma omnipresente dentro de la pila de seguridad promedio. Para tu PACS, siempre deberás tener que resolver problemas complicados y tendrás que estar bien preparado en áreas como selección de tecnología, integración, interoperabilidad, gestión de identidad, gestión de credenciales y acceso, ciberseguridad, rendimiento, confiabilidad, escalabilidad, cumplimiento normativo, capacitación de usuarios y, por supuesto, costos. Pero, espera, ¡hay más! Nuestra guía de mejores prácticas que ofrecemos en el Apéndice B son un punto de partida para el pensamiento estratégico y para la planificación de la adquisición de tecnología. Como siempre, es aconsejable consultar con un profesional confiable de la industria de la seguridad, como un distribuidor y/o integrador de tecnología. Desarrolla una gran cadena de suministro y úsala.

Sistemas de vigilancia

Sistemas de vigilancia

- Sistemas de seguridad por video
- Cámaras IR
- Cámaras con movimiento horizontal, vertical y zoom
- Cámaras termográficas
- Cámaras corporales
- Tecnología de reconocimiento de patrones
- Cámaras de reconocimiento facial
- Cámaras activadas por movimiento
- Sistemas de reconocimiento de placas vehiculares
- Sistemas de monitoreo remoto de video
- Sistemas de vigilancia y almacenamiento en la nube
- Analíticas de video
- Grabadores de video en red
- Drones y robots

Los sistemas de vigilancia son un recurso indispensable para monitorear e identificar amenazas potenciales. Permiten que una organización observe, disuada y reaccione ante posibles problemas en tiempo real mediante el uso de tecnologías como cámaras especialmente diseñadas, sistemas de grabación de video en red o monitoreo remoto, lo cual es fundamental. Poder verlo todo es un paso proactivo obvio en el proceso de maduración de una postura de seguridad física. Además, la tecnología está madurando y evolucionando en tal medida que estamos empezando a observar robots y drones con mayor frecuencia como parte de la huella de vigilancia.[15]

En las conversaciones sobre la implementación de sistemas de vigilancia, el almacenamiento de video debe ser parte de ellas. El almacenamiento a corto plazo y de archivo de datos de video es por lo general un elemento necesario del sistema, y el almacenamiento de grandes volúmenes de datos puede presentar algunos desafíos.[16] Pueden surgir problemas de compatibilidad y accesibilidad siempre que hablamos de datos. Más allá de las preocupaciones relacionadas con los grandes volúmenes de datos, también debemos considerar los requisitos de cumplimiento normativo, como la privacidad, y los problemas de confiabilidad, como la energía y la conectividad de la red.

No olvidemos que cada vez que surge el tema de los datos, también aparece el primo hermano de la seguridad: la ciberseguridad. Esa red que estábamos evaluando en cuanto a confiabilidad ahora necesita otro par de ojos que realicen análisis y pruebas. Disponible y operativo no es lo mismo que seguro.

Tener datos y poder utilizarlos tampoco es lo mismo. El acceso rápido y confiable a imágenes históricas es crucial, tanto para necesidades de investigación como forenses. El acceso basado en roles a los datos de video, la identificación de patrones y la obtención ocasional de evidencias para fines legales y de cumplimiento normativo permiten a las organizaciones tener una visión general de todas sus instalaciones y su viabilidad a futuro. Nunca asumas que tus valiosos datos de vigilancia ya se han puesto en funcionamiento y que ya aportan valor a tu negocio. Implementar el sistema correcto que responda a tus necesidades y te brinde valor no es tan simple, pero ciertamente es alcanzable.

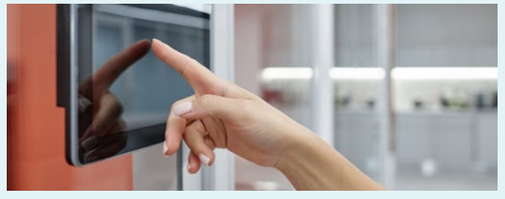
Digamos que lo hemos logrado. ¿Eso es todo? No. Simplemente instalar un excelente sistema de vigilancia en un edificio no siempre es un resultado valioso en sí mismo. Tener una capacidad real todavía requiere un poco más. ¿Y cuál es la estrategia correcta? ¿Están tus cámaras en los lugares correctos? Es fundamental identificar los principales objetivos de la vigilancia. ¿Cuáles son los puntos de acceso y los activos cruciales de tus instalaciones? ¿Están mapeados en tu plan? ¿Tienes un plan? ¿Tiene estrategias de crecimiento para tus sitios que sean congruentes con un plan tecnológico que las respalde? La implementación de sistemas de vigilancia escalables que se alineen con los requisitos de desarrollo organizacional ayuda a proporcionar continuidad de seguridad física a la infraestructura crítica a medida que las responsabilidades evolucionan inevitablemente.

Pero, espera, ¡hay más! Nuestros resultados importantes no se logran simplemente implementando las tecnologías correctas, de la manera correcta y con la estrategia correcta. Una verdadera capacidad requiere la combinación correcta de tecnología, procesos y personas para ser efectiva y aportar valor.

Lo primero que solemos pensar cuando pensamos en vigilancia es en alguien sentado detrás de un monitor, haciendo observaciones en tiempo real. Y, por supuesto, ese es un requisito básico. Y esto es, obviamente, por lo que llegamos a esto al último.

La efectividad del sistema de vigilancia no sólo está determinada por su tecnología subyacente, sino también por la accesibilidad al sistema por parte de las personas responsables de proporcionar resultados de seguridad. Sin personal adecuadamente capacitado para detectar y responder a las amenazas a la seguridad, el sistema sólo recopilará datos que posiblemente nunca se utilicen. La combinación de tecnología e interacción humana es fundamental para una sólida postura de seguridad física. ¿Se han puesto en funcionamiento tus grandes sistemas de manera apropiada para el uso humano? ¿Puede el sistema identificar de forma proactiva amenazas potenciales y proporcionar alertas al personal de seguridad, de ser necesario? ¿Son efectivos los sistemas y se adaptan a las necesidades de tu negocio y de tu equipo?

Sistemas de detección: Alarmas y sensores



Sistemas de detección (alarmas y sensores)

- Detección de patrones anómalos
- Alarmas inteligentes
- Radar y LiDAR
- Tecnología de geocercas
- Sensores sísmicos
- Dispositivos de pánico
- Detectores de humo y gas
- Detectores de agua, temperatura, calor y humedad
- Sensores de movimiento, vibración y manipulación
- Monitoreo acústico
- Sistemas de detección de drones
- Sensores magnéticos
- Sensores de presión y rotura de cristales
- Detectores de campo de microondas

Cuando pensamos en sistemas de detección, para los efectos de esta discusión nos ceñiremos al ámbito restringido de nuestra conversación, alineado con nuestro modelo de TSO. Nos enfocaremos principalmente en alarmas y sensores. Estos son dispositivos esenciales, pero a menudo olvidados, que se utilizan estratégicamente dentro de zonas de protección para identificar posibles amenazas, riesgos y violaciones. Cuando algo se sobrecalienta, nuestros detectores de calor lo detectan. Si algo comienza a moverse a través de un campo protegido, un sensor de movimiento lo detecta. Los sensores de presión proporcionan una sensación de tacto, los detectores de humo prácticamente pueden oler el humo y las señales de incendio, mientras que nuestros sensores de rotura de cristales nos permiten escuchar algo que puede ayudarnos a proteger la zona.

Imagina tu sistema de detección como la red sensorial del ecosistema de seguridad física: las partes que dan vida a nuestras capacidades. Pequeñas pero poderosas, nuestras alarmas y sensores son esenciales para el éxito de la misión. Cuando nuestros elementos de detección están adecuadamente orquestados dentro de una malla defensiva apropiada, podemos obtener una comprensión holística del

15 Drones domésticos. Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones (ACLU, 2025)
16 Diseño de sistemas de monitoreo de seguridad física para vigilancia y respuesta a la calidad del agua. Visto el 24 de enero de 2025. [Online]. Disponible en inglés: https://www.epa.gov/sites/default/files/2017-11/documents/esm_design_guidance_2017-11-02.pdf (EPA, 2017)

panorama de seguridad y desarrollar estrategias efectivas que mitiguen mejor los riesgos.[17]

Desde el punto de vista del diseño técnico, este tipo de tecnologías comparten algunas similitudes con los dispositivos del IoT, pero para ser claros, no son exactamente lo mismo. Ambos tienden a compartir paralelismos en estrategias de integración de computación en la nube y en el borde, monitoreo y comunicaciones en tiempo real, activadores basados en eventos y accesibilidad remota. Es importante comprender en qué difieren. En términos generales, los componentes de detección de seguridad cumplen una función única y pueden caracterizarse por diferentes dependencias de red, así como por capacidades limitadas de automatización y escalabilidad en comparación con los dispositivos del IoT comunes. También buscamos que nuestros sensores y alarmas de seguridad sean mucho menos accesibles universalmente para personas o sistemas paralelos que no cumplen ningún propósito en la misión de seguridad. Comprender qué componentes funcionan y cuáles no, y dónde y por qué, dentro de nuestra infraestructura operativa, nos ayudará a garantizar que se tomen las decisiones correctas durante la selección, implementación, mantenimiento, actualizaciones y mejoras de tecnología.

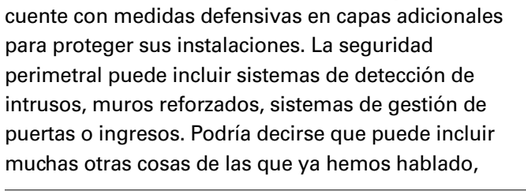
Cuando pensamos en los desafíos operativos relacionados con los dispositivos de detección, lo más común son las falsas alarmas. Desde un punto de vista técnico, imagínalo como una falla. Si no sucede con frecuencia, tenemos una molestia o una pequeña distracción. Si se vuelve más frecuente, puede transformarse en ruido blanco que puede elevar la probabilidad de riesgos de seguridad, incidentes o brechas en las defensas. Desde una perspectiva humana, imagínalo como el sensor que sigue quejándose. Las falsas alarmas generan complacencia y condicionamiento del personal a ignorar lo que eventualmente es una verdadera alarma; una que puede correr el riesgo de quedar sin respuesta.[18]

Hay muchas causas, pero algunas de las más comunes son errores humanos, problemas de integración e implementación, sensores mal posicionados, tecnología obsoleta, fallas del sistema, cortes de energía y falta de mantenimiento adecuado.[19] Trabajar con profesionales de integración de seguridad calificados puede ayudar a evitar muchos problemas de este tipo. Tus dispositivos de seguridad perimetrales requieren mantenimiento y pruebas regulares, pero a menudo se les resta prioridad. Con el tiempo muchas cosas pueden salir mal y la mayoría de estos elementos del sistema tienen una vida útil finita. Es aconsejable establecer capacidades de sistema de failover, redundancia y respaldo.

Siempre que sea posible, es mejor seleccionar tecnologías avanzadas capaces de reducir el ruido blanco de las falsas alarmas. Los sistemas de alto costo impulsados por funciones inteligentes e integraciones personalizadas suelen ser una barrera de entrada para muchas organizaciones, especialmente las PYMES. Para equilibrar las restricciones de costos, prioriza las áreas de alto riesgo que se encuentren en un mapeo físico inicial de la infraestructura de la empresa. No todos los sensores deben ser iguales. La uniformidad de los componentes no es un resultado. Pintar con una brocha ancha desde el nivel macro es innecesario cuando uno es profundamente consciente de sus micro necesidades y requisitos.

Si bien los sistemas de detección se utilizan a menudo para protegerse de riesgos humanos, también se utilizan para proteger diversas instalaciones de amenazas ambientales. El fuego, el viento y el agua pueden causar tanto daño o más que cualquier otra amenaza a la infraestructura de una empresa. Las condiciones climáticas, como los vientos fuertes, pueden crear falsas alarmas para los sensores de movimiento, alterar la ubicación o incluso destruir componentes mal colocados.[20] Es importante diseñar el ecosistema de malla de TSO con resiliencia contra amenazas externas únicas, manteniendo al mismo tiempo las capacidades necesarias para alertar con precisión al receptor previsto. La colocación de sensores no es tan sencilla como parece. Como primera línea de nuestro marco de admisión sensorial de seguridad física, los sistemas de detección de TSO desempeñan un papel único y crítico en la misión general. Hay mucho en juego para que esta parte salga bien. No dejes nada al azar.

Seguridad ambiental y perimetral (PES)



Seguridad perimetral y ambiental

- BMS
- Sistemas de respaldo de energía y comunicaciones
- Barreras y bolardos
- Soluciones de cercas
- Alambre de púas y de cuchillas
- Tecnologías de puertas
- Control de acceso de vehículos
- Trampas y vestíbulos de seguridad
- Torniquetes
- Cabinas de seguridad
- Iluminación, señalización y elementos disuasorios físicos
- Protecciones contra tormentas y ventanas de alta resistencia
- Barreras de drenaje y contra inundaciones
- Sistemas de contención

La creación de un perímetro físico alrededor de una instalación deja en claro a extraños lo que es público y lo que es privado. Los perímetros efectivos protegen contra intrusiones, vandalismo y accesos no autorizados de visitantes no autorizados. La implementación de soluciones de baja tecnología, como cercas y barreras, proporciona un elemento de material disuasorio y permite que una organización cuente con medidas defensivas en capas adicionales para proteger sus instalaciones. La seguridad perimetral puede incluir sistemas de detección de intrusos, muros reforzados, sistemas de gestión de puertas o ingresos. Podría decirse que puede incluir muchas otras cosas de las que ya hemos hablado, como PACS, tecnologías de vigilancia y sensores. Si bien esto es cierto, en esta sección estamos limitando el enfoque específicamente a los tipos de elementos que se encuentran en la Tabla 1, bajo la columna PES.

Al evaluar los distintos tipos de componentes del PES, la atención se centra en las barreras físicas y tecnológicas que retrasan, impiden o restringen los accesos no autorizados. Si bien estos dispositivos juegan un papel crucial en el ecosistema defensivo de seguridad física, debemos preguntarnos si en general encajan dentro de nuestra definición general de TSO. En concreto, ¿la TSO implica *únicamente* tecnologías digitales o electrónicas? Recordemos que definimos la TSO como:

> Los elementos técnicos subyacentes que nos permiten hacer nuestro trabajo como profesionales de la seguridad; tecnologías utilizadas para ayudarnos a respaldar, automatizar, escalar y entregar la misión principal de la seguridad física; la TSO ayuda a gestionar los problemas de seguridad y nos conecta con el mundo físico que intentamos proteger.

Para los fines de esta discusión, afirmaremos que sí. Nuestra atención se mantendrá en las partes electrónicas y conectadas digitalmente del dominio de la TSO, es decir, los elementos técnicos. Si bien soluciones como el alambre de púas, las cercas simples y las barreras desempeñan un papel importante en la seguridad, limitar nuestro debate permite mantener la narrativa consistente y centrada. Es más, esta subsección de la Tabla 1 puede ser una

17 7 componentes ambientales a tener en cuenta durante una auditoría de seguridad física. Visto el 25 de enero de 2025. [Online]. Disponible en inglés: https://www.security101.com/blog/7-environmental-components-to-take-in-consideration-during-a-physical-security-audit (Security 101, 2025)

18 Falsas alarmas de incendio. Visto el 27 de enero de 2025. [Online]. Disponible en inglés: https://www.firehouse.com/home/news/10545242/false-fire-alarms (Firehouse, 1996)

19 3 consejos para ayudar a reducir el riesgo de falsas alarmas. Visto el 27 de enero de 2025. [Online]. Disponible en inglés: https://www.adtsecurity.com.au/blog/security-tips-community/risk-of-false-alarms (ADT, 2025)

20 7 formas de prevenir falsas alarmas en tu sistema de seguridad. Visto el 27 de enero de 2025. [Online]. Disponible en inglés: https://adssecurity.com/prevent-false-alarms-with-your-security-system (Vector Security, 2021)

zona gris de la discusión, debatible y subjetiva según el punto de vista específico de cada uno.

En ese sentido, comenzaremos con uno de esos puntos discutibles, es decir, la categorización del sistema de gestión de edificios (BMS) como un elemento del PES. Algunos podrían argumentar que el BMS está más apropiadamente alineado con nuestra siguiente sección, la categoría de gestión de seguridad de la Tabla 1. Pero nuestra afirmación es que la misión principal de un BMS es gestionar los sistemas de calefacción, ventilación y aire acondicionado, energía e iluminación dentro de un edificio.[21] El enfoque clave del BMS está relacionado con la gestión de los controles ambientales dentro de un espacio comercial. El BMS es una herramienta y también una tecnología operativa. Con el tiempo, los sistemas de BMS han evolucionado para desempeñar un papel importante en la misión de seguridad al ayudar a integrar, automatizar y escalar una variedad de componentes de sistemas de seguridad física, contra incendios y protección de la vida dentro de un espacio de un edificio comercial.[22] De esta manera, se aprovechan los BMS para brindar capacidades de TSO para respaldar el entorno del edificio en general. Por lo tanto, consideramos que el BMS es un elemento de nuestro PES porque nos permite realizar nuestro trabajo como profesionales de la seguridad y sirve para ayudarnos a respaldar, automatizar, escalar y cumplir la misión principal de la seguridad física. También resulta ser una tecnología clave para la seguridad, ya que proporciona un conducto o un sistema de autopistas para todo el entorno designado para la protección.[21]

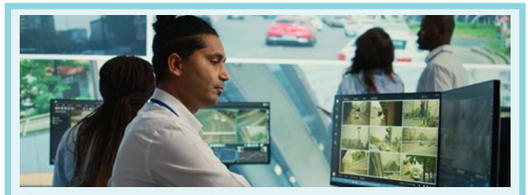
Sin embargo, los propietarios de instalaciones, los líderes de PYMES y los técnicos de seguridad física no suelen estar acostumbrados a trabajar con un BMS y algunos de sus matices les sorprenden.[23] Por ejemplo, no es raro descubrir que las plataformas de BMS pueden presentar grandes desafíos en lo que respecta a la integración. Un BMS se puede caracterizar por componentes y protocolos propietarios que no se conectan fácilmente a tu TSO. Generalmente hay que lidiar con tecnologías antiguas, problemas de compatibilidad e incluso limitaciones de escalabilidad. Pueden existir problemas de ciberseguridad y cumplimiento relacionados con protocolos de un BMS frecuentemente utilizado e inseguro, como BACnet y Modbus. Los desafíos no son irresolubles, y las ventajas de aprovechar un BMS para brindar mejores resultados de seguridad y dar un soporte consistente valen la inversión en términos de ahorro a largo plazo.

Siempre que sea posible, es muy deseable desarrollar la complejidad de los datos y la información para convertirlos en soluciones más fácilmente consumibles. Puede resultar conveniente considerar capacidades que integren todas tus plataformas de BMS en un "panel único" de fácil acceso. Esto proporciona a los operadores información sobre todos sus sistemas, de forma sencilla e inmediata. Jay Williams, Vicepresidente de Ventas de Infraestructura de Red en Wesco, afirma: "Estamos descubriendo que, a medida que la cantidad de TSO y otras plataformas continúa creciendo, las organizaciones buscan soluciones que les ayuden a conectar, recopilar, analizar y actuar sobre esos flujos de datos dispares desde una sola pantalla."

Proporcionar un entorno estable para las instalaciones de una organización puede aumentar la productividad. También es un factor de éxito para las TSO primarias, como los PACS, los sistemas de vigilancia y los sensores. Pensemos por un momento en la iluminación. Puede que para muchos no parezca un componente de TSO. Pero sin duda desempeña varias funciones esenciales. Pensemos por un momento en la iluminación como un elemento secundario de seguridad, necesario para que el personal de seguridad sea efectivo como individuos y que también puede ser necesario para garantizar la efectividad de muchos sistemas de videovigilancia.[24] Hay un tercer ejemplo de la utilidad de la iluminación para la seguridad. La creación de un entorno iluminado constantemente apoyará directamente la misión de seguridad al disuadir posibles amenazas criminales. Mantener un espacio protegido con un aspecto ocupado, activo y vivo puede crear un objetivo menos intrigante para posibles atacantes.

Los elementos PES tienen un papel fundamental dentro de la postura general de madurez de seguridad de un sitio. Comprender e identificar qué son suele ser una tarea ilusoria no sólo para las PYMES, sino también para las empresas más grandes. Uno no piensa en cómo las comunicaciones, los sistemas de energía y la automatización de edificios están intrínsecamente conectados a la misión de seguridad, hasta que algo sale mal. Tener el plan correcto comienza con ver todo el campo de batalla. Y cuando las tecnologías de acceso automatizado y las cabinas de seguridad se conectan digitalmente a tu ecosistema de seguridad más amplio, el mismo pensamiento, estrategia y planificación discutidos anteriormente se aplicarán también a tus elementos PES. También será necesario deliberar sobre el desarrollo de requisitos funcionales, la selección de tecnología, la implementación, la integración y las consideraciones de soporte y mantenimiento del ciclo de vida, ya que se aplican también a estos elementos matizados del recorrido de madurez de la seguridad. Una vez más, las cosas no siempre son tan fáciles como parecen a primera vista, por lo que es recomendable consultar con un profesional confiable de la industria de la seguridad, como un distribuidor y/o integrador de tecnología.

Gestión de la seguridad



Gestión de la seguridad

- Centro de operaciones de seguridad física
- Monitoreo remoto
- Tecnología de analíticas de video
- Sistemas de notificación de incidentes
- Sistemas de notificación masiva
- Sistemas de torres de vigilancia
- Dispositivos de comunicación
- Sistemas PA
- Sistemas de detección y extinción de incendios
- Sistemas de salida de emergencia
- Plataformas de seguridad integradas
- Dispositivos de seguridad del IoT
- Capacidades de ciberseguridad
- Rastreo GPS

La gestión de la seguridad abarca una amplia gama de TSO destinadas a conectar, proteger y optimizar. Los resultados importantes giran en torno a permitir que las organizaciones proporcionen una función de gestión de amenazas centralizada en tiempo real, junto con un amplio soporte y respuesta. El tema común aquí es la escalabilidad. La administración de complejas TSO integradas a menudo requiere que se envíe a campo un conjunto de trabajadores capacitados para comprender, optimizar y poner en funcionamiento una variedad de tecnologías, datos y situaciones de alta presión. Encontrar formas de automatizar parte de ese trabajo es muy valorado. La creación de un centro de operaciones de seguridad física (PSOC) es un ejemplo principal de una estrategia que emplean las grandes corporaciones para proteger instalaciones a gran escala. Los PSOCs brindan a las organizaciones la capacidad de consolidar grandes conjuntos de datos que fluyen desde una red de dispositivos de TSO y dar un enfoque de panel único para gestionar las amenazas de manera más económica, consistente y eficiente.

Pero a menudo, cuando la gente considera la idea

21 ¿Qué es un sistema de gestión de edificios? Visto el 10 de enero de 2025. [Online]. Disponible en inglés: https://www.cim.io/blog/what-is-a-building-management-system (CIM, 2025)

22 Cómo la integración de sistemas de seguridad con un BMS puede ayudar a mejorar la seguridad de la propiedad comercial. Visto el 10 de febrero de 2025. [Online]. Disponible en inglés: https://stealthmonitoring.com/crime-prevention/how-integrating-security-systems-with-bms-can-help-elevate-commercial-property-security (Stealth Monitoring, 2025)

23 El desafío de proteger los sistemas de gestión de edificios, E. Ben-Meir. Visto el 3 de febrero de 2025. [Online]. Disponible en inglés: https://www.techtarget.com/iotagenda/blog/IoT-Agenda/The-Challenge-Of-Securing-Building-Management-Systems (TechTarget, 2019)

24 Iluminando el camino hacia una ciudad más inteligente y segura. Visto el 31 de enero de 2025. [Online]. Disponible en inglés: https://www.securityindustry.org/2018/09/14/lighting-the-way-to-a-smarter-safer-city/ (SIA, 2018)

de un PSOC, o escucha las palabras "centro de operaciones de seguridad", imaginan una sala enorme con pantallas en todas las paredes, como si fuera el control de misiones de la NASA. Se imaginan torres de computadoras del tamaño de una camioneta y escritorios alineados en habitaciones oscuras, con operadores de seguridad ocupando cada asiento, intentando rápidamente resolver problemas complejos y comunicándose con figuras oscuras como Jack Bauer. Para la PYME promedio, la idea de un PSOC puede parecer un poco exagerada. Pero no es así.

Imagínalo simplemente como software, porque eso es realmente todo lo que se necesita. Cualquiera que busque la seguridad junto con limitaciones de presupuesto y una computadora portátil está en un camino viable en este viaje.[25] Todo lo necesario para el PSOC estándar se puede adquirir por tan sólo unos pocos cientos de dólares al mes en tarifas de licencias totales. Algunos de los elementos básicos basados en software incluyen:

- Software de centro de comando y respuesta a incidentes
- Software de control de acceso y autenticación electrónica
- Software de vigilancia y gestión de video
- Software de gestión de alarmas y detección de intrusiones

Claro, todo eso puede parecer muchas cosas sofisticadas. Pero no es tan inaccesible como parece. La buena noticia es que probablemente ya tengas la mayoría de las piezas. Por ejemplo, muchos de los sistemas de control de acceso electrónico más destacados, que son un elemento fundamental de tu pila de PACS, incluyen software de autenticación y control de acceso electrónico. Suena obvio, ¿verdad? Es muy probable que el software de gestión de video y vigilancia ya sea parte de tu sistema de grabación de video en red. Y aunque carezcas de estos elementos, no es tarea difícil.

La clave del viaje del PSOC es la democratización de los datos. La integración con un BMS permite habilitar capacidades centralizadas más ricas. La conclusión fundamental es que este es un resultado posible para las PYMES. Otras soluciones livianas y económicas, como aplicaciones de monitoreo móvil que pueden entregarse a un teléfono inteligente, brindan mayores niveles de escalabilidad, efectividad y capacidad de soporte para cualquier responsable de instalaciones con presupuesto limitado. Las estrategias y competencias del PSOC no son dominio exclusivo del uno por ciento corporativo. Hay soluciones para la mayoría de los presupuestos.

La gestión de la seguridad nos conduce hacia un único resultado común: comprender y gestionar el panorama general. Esta categoría de TSO representa los elementos que consumen y dan funcionalidad a grandes conjuntos de datos, crean conciencia masiva, valor y brindan resultados integrales de base amplia. Las capacidades de ciberseguridad son un ejemplo y un ingrediente integral de un panorama más amplio. Nos gusta decir que es primo hermano de la seguridad física. Las instalaciones y los sistemas de los edificios no son seguros cuando no son ciberseguros. Como alguna vez lo dijo una persona sabia, hay que ser proactivo e involucrar desde el principio a expertos en tecnología y dominios de seguridad. Los CISOs y CIOs son tus amigos.

Éstos son los elementos de TSO de alto impacto, en términos de resultados. Los sistemas de notificación masiva garantizan que las partes interesadas puedan transmitir y recibir alertas críticas cuando sea necesario, a gran escala. Las organizaciones con capacidad para dirigir y comandar grandes multitudes de manera efectiva tienen una ventaja en la gestión de crisis y en las operaciones cotidianas. El intercambio rápido de datos, la conectividad y la integración con otros elementos críticos del ecosistema de seguridad, como seguridad humana, sistemas contra incendios, componentes de seguridad y otras TSO primarias, aumentan la eficiencia y reducen el riesgo.[26]

25 El mejor software de seguridad física. Visto el 1 de febrero de 2025. [Online]. Disponible en inglés: https://www.softwareworld.co/physical-security-software/ (SoftwareWorld, 2025)
26 Los beneficios de la integración de la seguridad contra incendios, la protección de la vida y la seguridad, T. Giannini. Visto el 4 de febrero de 2025. [Online]. Disponible en inglés: https://www.buildings.com/industry-news/article/10189775/the-benefits-of-fire-life-safety-and-security-integration (Buildings, 2012)

Existen diversas aplicaciones y propósitos cuando pensamos en los componentes de TSO de gestión de seguridad. Si ampliamos nuestro alcance de pensamiento a todos los diferentes tipos de TSO y luego integramos cada uno, creando radios interdependientes dentro de una máquina de seguridad, un PSOC podría considerarse como el centro. Eso es lo que lo hace útil y éste es el verdadero valor del pensamiento de gestión de seguridad. Por más complejo que pueda ser cada elemento del ecosistema de seguridad, unirlo todo para ofrecer una plataforma centralizada es posible, pero no tan sencillo.

Como sucede con todas las subsecciones de nuestro panorama general de TSO, las tecnologías de gestión de seguridad requieren mucha reflexión, deliberación y planificación. Y si bien algunos proveedores de tecnología puedan sugerir opciones de "hazlo tú mismo" para las PYMES, reiteraremos que las cosas no son tan simples como parecen. Consolidar todas las complejidades de tus sistemas de TSO con las estrategias y tecnologías adecuadas que respondan a tus necesidades y prioridades empresariales individualizadas es un objetivo final alcanzable. Para lograr escalabilidad y brindar un alto valor con recursos limitados se necesita una amplia comprensión de las opciones técnicas, la planificación adecuada, el conocimiento del dominio, la integración, la capacidad del personal y el mantenimiento y soporte continuos. La gestión de la seguridad consiste en mantener efectivas y sostenibles las capacidades de tu misión. Vale la pena hacerlo bien, y ninguno de los muchos desafíos es insuperable. Desarrolla tu plan, utiliza tus recursos y asociaciones y ejecuta bien. Recuerda siempre que el trabajo de seguridad y desarrollo de TSO no es un estado finito. Las amenazas evolucionan y tu estrategia también debe hacerlo.

Conclusión

Grandes cosas suceden cuando las partes interesadas se comunican bien y se entienden entre sí. Ya sea que seas un experto, profesional, técnico o integrador de la industria de seguridad, o si estás en la cadena de suministro, o eres el responsable de una PYME que busca TSO, el entendimiento mutuo del espacio operativo, los desafíos y la capacidad relativa para facilitar, entregar, consumir y dar soporte lo será todo. Comprar herramientas costosas en el ámbito de las TSO no es una solución al problema. Simplemente se necesita más.

Todo escalador o aventurero primerizo necesita de un guía capaz. Si eres una PYME consumidora de TSO, nunca es una buena idea iniciar esta compleja tarea sin antes consultar a tus expertos de confianza: tu profesional de seguridad, distribuidor de tecnología, integrador o proveedor. A veces, el objetivo de economizar se logra tomando las decisiones iniciales correctas y realizando inversiones inteligentes que generen ahorros en los costos del ciclo de vida. Pensar a largo plazo puede resultar menos perjudicial para tu negocio y ser más sostenible, además de generar mejores resultados en materia de seguridad. Todo se reduce al plan adecuado.

Si eres un profesional de la industria de la seguridad cuya misión es ser ese guía confiable en el recorrido de las TSO, comprender las necesidades de tu cliente, los resultados reales deseados y los requisitos completos del ciclo de vida es tan importante como la experiencia en el dominio técnico. La comprensión mutua de lo que significa la victoria, lo que se necesita para llegar a ella y qué problemas estamos tratando de resolver ayudará a garantizar el éxito mutuo.

Ya sea que se implemente una TSO en particular por primera vez, se migre a uno nuevo o se mejore uno antiguo, las preguntas importantes deben girar en torno a los resultados, la estrategia, la planificación, la selección de herramientas y los detalles de la integración, la entrega y el soporte del ciclo de vida. Todas las partes necesitan concientización, pero desgraciadamente, a menudo no la tienen. Muchas empresas y organizaciones priorizarán la implementación del nuevo sistema para resolver el

problema del día, mientras descuidan la planificación del mantenimiento a largo plazo y el soporte del ciclo de vida.[27] Hacerlo bien es responsabilidad de todos.

No es raro cometer el error de creer que adquirir la nueva y brillante solución de TSO es el destino, en lugar de sólo el comienzo del viaje. Es parte de la naturaleza humana asumir que el resto del trabajo será fácil de entender una vez que tengamos las herramientas que puedan poner en funcionamiento de manera efectiva los requisitos de nuestra misión. Una capacidad requiere más que sólo la tecnología subyacente. Poseer máquinas para cortar el césped no significa que éste luzca bonito. Una TSO rara vez aportará valor de forma independiente. Se requiere más y la receta adecuada para el éxito varía para cada negocio.

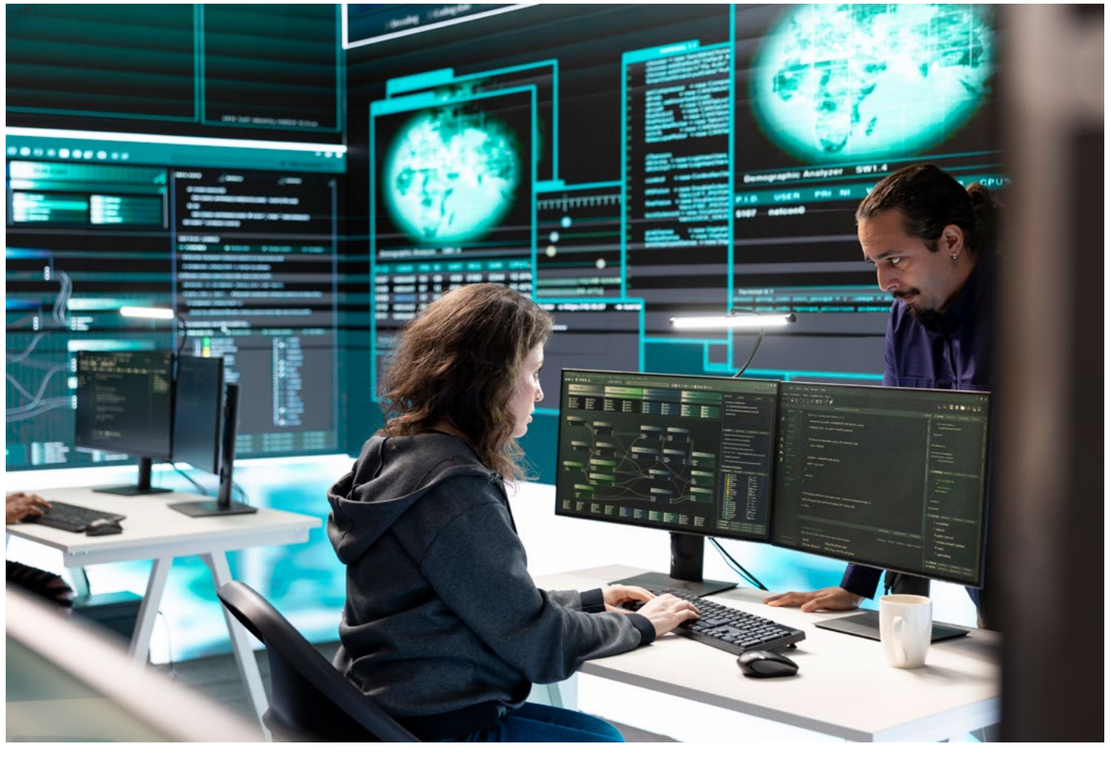
El análisis, la evaluación y la preparación son parte integral del inicio de cualquier proyecto enfocado en instituir o mejorar las capacidades de seguridad. La puesta en funcionamiento de una TSO nueva o el mantenimiento de una existente requiere más que las promesas de los fabricantes de equipos originales y los proveedores. Muchas de estas tecnologías son complicadas de integrar y mantener. Un plan interno de recursos y apoyo es esencial para el éxito. Las asociaciones sólidas con terceros son ventajosas. Siempre habrá necesidades de mejora, progreso y avance al aprovechar la TSO destinada a resolver problemas humanos o físicos. Sé proactivo y ten un plan.

Considerando la realidad de que las necesidades y requisitos operativos de seguridad no suelen ser estáticos y, por el contrario, continúan evolucionando,[28] debemos reconocer que nuestros elementos de TSO requieren atención continua y apoyo dinámico. A medida que avances como la IA y el aprendizaje automático continúan evolucionando y van surgiendo nuevas tecnologías, también lo harán los riesgos asociados y la atención que deberemos aplicar a nuestra misión crítica de TSO.[29] A veces, los avances, como una nueva entrega en la nube de tecnologías de seguridad tradicionalmente locales, pueden introducir dificultades y brechas de soporte para las que tu fabricante de equipos originales puede no haberte preparado. Nuestra infraestructura y ecosistema institucional de TSO deben estar diseñados para adaptarse a nuestras necesidades personalizadas.

Reconocer quiénes somos y dónde operamos nos ayudará a protegernos contra implementaciones problemáticas de TSO. Es necesario responder a preguntas fundamentales antes de lanzarse a la lucha por resolver el problema del día y comprometerse con un gasto de capital considerable, sin comprender el panorama general, los costos ocultos y los costos operativos potencialmente considerables que se avecinan. Todo cambia. ¿Puede tu enfoque institucional volverse dinámico o estás operando dentro de un entorno estático que cambia lentamente? La historia habitual que cuentan muchos operadores de seguridad es que carecen de tiempo para impulsar mejoras, pero son conscientes de las brechas.[30]

Para dimensionar, alinear y mejorar la propia pila tecnológica de seguridad se requiere un enfoque estricto en los resultados operativos y la disciplina y objetividad para buscar oportunidades constantemente. Comunicar efectivamente los beneficios y el valor de las iniciativas de seguridad a los que toman las decisiones, que controlan el dinero y tienen la autoridad para actuar, es todo un arte. Pero los ingredientes necesarios están conectados a los datos, al contexto y a la alineación con los objetivos de la organización, empresa o institución. La mejora o introducción de una TSO debe manejarse con cuidado y planificarse de acuerdo con el panorama general y un conocimiento profundo del conjunto completo de factores predominantes.

El dominio de las TSO es una red compleja de desafíos y dificultades, pero ninguno es insuperable y los resultados de seguridad al final del recorrido bien valen las inversiones necesarias. Proteger a las personas, la propiedad y los recursos valiosos es un objetivo noble. Pero no es sencillo. Al trabajar juntos y compartir nuestras valiosas experiencias y conocimientos del dominio, podemos garantizar el éxito mutuo mediante la elaboración de estrategias colaborativas y la resolución de los desafíos para garantizar mejor la entrega óptima y las mejores prácticas operativas.



27 Encuesta de PwC sobre tendencias digitales en operaciones en 2024: Por qué aún es difícil lograr resultados comerciales significativos y qué puedes hacer. Visto el: 9 de noviembre de 2024. [Online]. Disponible en inglés: https://www.pwc.com/us/en/services/consulting/business-transformation/digital-supply-chain-survey.html (PwC, 2024)
28 El riesgo es dinámico, por lo que la evaluación del riesgo físico debe ser continua, D. Young, M. Martin. Visto el: 1 de diciembre de 2024. [Online]. Disponible en inglés: https://www.asisonline.org/security-management-magazine/articles/2023/11/dynamic-risk-assessment/continuous-physical-risk-assessment (ASIS, 2023)
29 Los 15 mayores riesgos de la inteligencia artificial, B. Marr. Visto el: 1 de diciembre de 2024. [Online]. Disponible en inglés: https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence (Forbes, 2023)
30 8 desafíos que enfrenta todo centro de operaciones de seguridad, J. Burke. Visto el: 1 de diciembre de 2024. [Online]. Disponible en inglés: https://www.techtarget.com/searchsecurity/tip/8-challenges-every-security-operations-center-faces (Tech Target, 2020)

APÉNDICES

Esta colección de materiales de referencia proporciona orientación sobre muchas de las mejores prácticas que podrían aplicarse para la planificación estratégica relacionada con las TSO. Este contenido se ofrece como una guía para comenzar a explorar más a fondo los temas de este documento.

El contenido proporcionado en estos apéndices (A, B y C) se basa únicamente en la investigación, el conocimiento personal y la experiencia de los autores. Gran parte del contenido de esta sección proviene de estándares comunes de la industria y de fuentes disponibles públicamente. Este documento tiene únicamente fines informativos y no debe interpretarse como asesoramiento exhaustivo o definitivo. Si bien se ha hecho todo lo posible para garantizar la precisión de la información, los autores no pueden garantizar que se hayan cubierto todas las posibles soluciones o escenarios. El uso de la información proporcionada queda a tu propia discreción y riesgo. SIA, los autores y cualquier parte asociada niegan cualquier responsabilidad por daños o pérdidas incurridos como resultado de la aplicación o confianza en el contenido aquí incluido. Te recomendamos buscar orientación profesional adaptada a tu situación específica.

APÉNDICE A:

Material de referencia destacado relacionado con las TSO y la seguridad física

NIST SP 800-82r3

Este documento proporciona orientación sobre cómo proteger las tecnologías operativas y al mismo tiempo abordar sus requisitos únicos de rendimiento, confiabilidad y seguridad. Las TO incluyen sistemas y dispositivos programables que interactúan con el entorno físico o gestionan dispositivos que lo hacen.

NIST 800-12 Capítulo 15

Este capítulo analiza los beneficios de las medidas de seguridad física y presenta una descripción general de los controles de seguridad física y ambiental comunes.

Seguridad física CISA

La Agencia de Seguridad Cibernética y de Infraestructura (CISA) proporciona acceso a herramientas y recursos que respaldan la seguridad física y la resiliencia. Se coordina con las partes interesadas y los expertos para brindar recomendaciones sobre medidas de protección para organizaciones de todos los tamaños.

Integración de seguridad de la North American Electric Reliability Corporation (NERC)

Este documento proporciona información sobre cómo proteger la red eléctrica durante su rápida transformación, enfocándose en los esfuerzos de ciberseguridad para los recursos energéticos distribuidos (DER) y los agregadores de DER.

Lineamientos de seguridad física del centro de datos

Este documento (en inglés) describe las mejores prácticas para proteger los centros de datos y la infraestructura física que almacenan, procesan y transmiten datos confidenciales.

Centro nacional de estadísticas de educación

Este recurso (en inglés) cubre las medidas de seguridad para las instituciones educativas y describe protocolos para proteger los datos de los estudiantes, los sistemas de TI y las instalaciones de los campus contra amenazas.

Principios de la ciberseguridad de la tecnología operativa

Este documento (en inglés) presenta seis principios para orientar a los tomadores de decisiones de la TO con el fin de garantizar que las decisiones de ciberseguridad no afecten negativamente a los entornos de la TO.

Mejores prácticas para la planificación y gestión de recursos de seguridad física: Una guía del Comité de Seguridad Interinstitucional

Una guía (en inglés) del Comité de Seguridad Interinstitucional que proporciona estrategias para la asignación de recursos de seguridad física, la evaluación de riesgos y la inversión en infraestructura de seguridad.

Protege la seguridad física de tus dispositivos digitales

Una guía (en inglés) de la CISA que describe los pasos para proteger dispositivos móviles, computadoras portátiles y otros activos digitales contra robos, accesos no autorizados y manipulación.

Consejos de concientización sobre seguridad de OSY/OCIO

Este documento (en inglés) proporciona capacitación en concientización sobre seguridad y las mejores prácticas para prevenir accesos no autorizados, amenazas internas y filtraciones.

Mejores prácticas de ciberseguridad

Un marco (en inglés) de la CISA que combina las mejores prácticas de ciberseguridad y seguridad física, incluida la gestión de contraseñas, la autenticación de múltiples factores y las auditorías de seguridad.

Uso de la seguridad operacional (OPSEC) para respaldar una cultura de ciberseguridad en entornos de sistemas de control

Orientación para la integración de los principios OPSEC en las políticas de ciberseguridad dentro de sistemas de control críticos, como redes eléctricas y automatización industrial (documento en inglés).

Seguridad de las Operaciones del Departamento de Defensa de EE.UU.

El Departamento de Defensa de EE.UU. proporciona estrategias de OPSEC que abarcan la gestión de riesgos, la protección de datos confidenciales y los protocolos de seguridad militar (documento en inglés).

Guía del estudiante de introducción a la seguridad física

Una guía (en inglés) que cubre medidas fundamentales de seguridad física, incluida la defensa del perímetro, los sistemas de control de acceso y la planificación de respuesta a emergencias.

Estándares y mejores prácticas de evaluación de seguridad física en los campus de educación superior de Tennessee

Medidas de seguridad diseñadas para proteger a las instituciones de educación superior, garantizando la seguridad del campus, la preparación para emergencias y la mitigación de riesgos.

Programa de ciberseguridad del HHS

Un programa del Departamento de Salud y Servicios Humanos de EE.UU. que proporciona las mejores prácticas para proteger los registros médicos electrónicos, los dispositivos médicos y las redes hospitalarias (documento en inglés).

Lineamientos de seguridad física para el sector eléctrico

Una guía (en inglés) de la NERC sobre cómo proteger plantas de energía, subestaciones y centros de control de energía del acceso no autorizado y las amenazas cibernéticas.

Lineamientos de seguridad física de centros de datos

Una guía (en inglés) que cubre las mejores prácticas para la seguridad física de los centros de datos. El proyecto Open Compute proporciona una descripción técnica general que ofrece orientación para servidores individuales y campus con varios edificios.

Documento de certificación de seguridad de la información global

Un documento técnico (en inglés) sobre las mejores prácticas de seguridad física, que incluye evaluación de riesgos, auditorías de seguridad y planificación de respuesta a incidentes.

Mejores prácticas del Programa de Ciberseguridad del Departamento de Trabajo de EE.UU.

Este documento (en inglés) ofrece las mejores prácticas para la protección de datos, la seguridad física de los activos de TI y la mitigación de amenazas internas para agencias gubernamentales y empresas privadas.

Descripción general de las medidas de seguridad física – Centro nacional para la seguridad escolar

Un documento (en inglés) de planificación para la seguridad escolar, que incluye preparación para emergencias, infraestructura de seguridad y medidas de protección para estudiantes y profesores.

Manual de diseño de seguridad física para instalaciones de misión crítica del VA

Una publicación (en inglés) del Departamento de

Asuntos de Veteranos (VA) sobre cómo proteger instalaciones gubernamentales de misión crítica, incluidas estrategias de seguridad para hospitales, centros de datos y oficinas.

Programa de seguridad física: Acceso a las instalaciones del Departamento de Defensa

Una guía de seguridad del Departamento de Defensa de EE.UU. que describe las políticas de control de acceso de seguridad física para instalaciones militares, centrándose en credenciales, zonas restringidas y respuesta a emergencias (documento en inglés).

APÉNDICE B:

Mejores prácticas de TSO

La información de esta sección debe utilizarse como material de referencia que proporcione una guía generalizada de mejores prácticas relacionadas con la tecnología operativa en el ámbito de la seguridad física. Revisa el Apéndice A para obtener materiales relevantes en este espacio que te permitirá desarrollar una comprensión más profunda.

Selecciona ideas estratégicas para adquirir o actualizar TSO

Selección de tecnología

- Define objetivos claros: Identifica los problemas específicos que la TSO debe resolver antes de evaluar las opciones.
- Utiliza una matriz de requisitos: Crea una lista de control de requisitos funcionales y no funcionales vinculados a los objetivos comerciales.
- Alineación de las partes interesadas: Realiza talleres con todas las partes interesadas para garantizar el consenso.
- Análisis del impacto empresarial: Evalúa cómo la TSO se alinea con los indicadores clave de rendimiento.
- Marco de selección de tecnologías: Desarrolla un sistema de puntuación basado en características críticas, escalabilidad y rentabilidad.
- Consulta a expertos de la industria: Contrata consultores o socios de la industria.
- Pruebas piloto: Lleva a cabo pruebas de concepto para comparar diferentes soluciones en escenarios del mundo real.
- Reseñas de clientes y casos de estudio: Observa los comentarios de usuarios reales y las tasas de adopción de la industria para filtrar productos impulsados por la publicidad. Solicita referencias de clientes a los fabricantes de equipos originales (OEMs).
- Análisis del costo total de propiedad: Incluye los costos de licencia, capacitación, mantenimiento y actualización en la planificación de presupuesto.
- Elige soluciones escalables: Selecciona tecnologías modulares o basadas en la nube que crezcan con las necesidades del negocio.
- Pronósticos del retorno de la inversión: Compara las posibles ganancias de eficiencia con la inversión inicial para justificar los costos.
- Utiliza los modelos de suscripción (SaaS): Reduce los gastos de capital optando por modelos de precios de pago por uso.
- Elige estándares abiertos: Prioriza soluciones que respalden estándares industriales ampliamente aceptados
    - Por ejemplo: El Protocolo de Dispositivo Supervisado Abierto (OSDP) de SIA y ONVIF pueden garantizar un equilibrio entre seguridad e interoperabilidad. Evita los protocolos propietarios.
- Soluciones de middleware: Implementa puertas de enlace API o plataformas de middleware para conectar sistemas incompatibles.
- Plataformas de integración basadas en la nube: Utiliza tecnologías nativas de la nube que ofrezcan una integración flexible con otros servicios, cuando y donde sea conveniente.
- Evaluación de proveedores: Confirma las capacidades de integración antes de la compra y prueba la interoperabilidad en un entorno sandbox.
- Adopta arquitecturas modulares: Selecciona soluciones que permitan una fácil expansión o personalización.
- Soluciones nativas de la nube y basadas en microservicios: Asegúrate de que la tecnología

que elijas soporte el escalamiento elástico.

- Considera las hojas de ruta de los proveedores: Evalúa la viabilidad a largo plazo de una tecnología revisando la línea de innovación de los proveedores.
- Modelos híbridos: Utiliza una combinación de soluciones locales y en la nube para equilibrar el control y la escalabilidad, cuando y donde tenga sentido.
- Enfoque de seguridad primero: Evalúa el cifrado, los mecanismos de autenticación y las certificaciones de cumplimiento (por ejemplo, ISO 27001, SOC2, GDPR).
- Auditorías de seguridad de terceros: Realiza pruebas de penetración y evaluaciones de riesgos antes de la implementación.
- Control de acceso basado en roles (RBAC): Implementa permisos de acceso detallados para minimizar los riesgos de seguridad.
- Listas de control del cumplimiento normativo: Asegura la alineación con los estándares de la industria.
- Diseño centrado en el usuario: Selecciona tecnología con una interfaz/experiencia de usuario intuitiva para reducir la curva de aprendizaje.
- Elige tecnologías de código abierto o de estándar abierto: Evita depender de un proveedor seleccionando soluciones interoperables.
- Estrategia de múltiples proveedores: Evita depender de un solo proveedor diversificando tus proveedores de tecnología.
- Acuerdos de nivel de servicio (SLA): Negocia contratos flexibles con proveedores para asegurarte un soporte continuo.
- Planificación de una estrategia de salida: Establece un plan de migración para datos y aplicaciones.
- Pruebas comparativas: Realiza pruebas de estrés y evaluaciones de rendimiento antes de la implementación completa.
- Estrategias de redundancia y failover en la nube: Asegura la disponibilidad a través de instancias de nube redundantes.
- Garantías de tiempo de actividad del servicio: Elige proveedores con acuerdos de nivel de servicio altos (compromisos de tiempo de actividad del 99,99% o más).
- Marco de toma de decisiones ágil: Utiliza metodologías como RACI para aclarar los roles de decisión.
- Establece plazos claros: Define plazos de decisión para evitar evaluaciones prolongadas.
- Análisis de riesgo versus recompensa: Utiliza modelos de puntuación ponderada para evaluar las opciones de forma objetiva.
- Programas piloto: Implementa pruebas a pequeña escala antes del compromiso total para mitigar los riesgos.

Costo

- Prioriza las áreas de alto riesgo: Comienza por actualizar la TSO en las ubicaciones más sensibles antes de expandirla a todo el sistema.
- Análisis del costo del ciclo de vida: Evalúa el costo total de propiedad a lo largo del tiempo para evitar gastos ocultos.
- Subvenciones e incentivos: Explora las subvenciones gubernamentales o de la industria que apoyan mejoras en la seguridad electrónica.

Integración e interoperabilidad

- Estándares abiertos: Elige una TSO que soporte protocolos abiertos, como SIA OSDP, para garantizar un equilibrio entre seguridad e interoperabilidad. Evita los protocolos propietarios.
- Sistemas basados en API: Selecciona una TSO con APIs robustas que permitan la integración con plataformas de seguridad de terceros.
- Middleware: Implementa middleware para que actúe como un puente entre la infraestructura de seguridad antigua y la moderna.
- Sistemas basados en la nube: El uso de soluciones de seguridad basadas en la nube puede optimizar la integración entre múltiples sistemas y ubicaciones. Pero asegúrate de que una solución SaaS se ajuste a tus necesidades y soporte tu implementación.

Confiabilidad

- Compatibilidad con modo sin conexión: Implementa una TSO que permita que las puertas y los puntos de acceso funcionen en modo sin conexión si la red falla.
- Soluciones de energía de respaldo: Asegúrate de que la TSO tenga un suministro de energía ininterrumpida para mantener las operaciones durante los cortes.
- Arquitectura redundante: Implementa servidores de failover y toma de decisiones de control de acceso descentralizada para evitar tiempos de inactividad.
- Mantenimiento y pruebas regulares: Programa controles del estado del sistema y mantenimiento preventivo para identificar posibles problemas antes de que ocurran fallas.

Cumplimiento regulatorio

- Implementa una TSO basada en el cumplimiento: Utiliza sistemas que soporten el acceso basado en roles, registros de auditoría e informes de cumplimiento normativo.
- Políticas de retención de datos: Asegúrate de que los registros de acceso se almacenen de forma segura y cumplan con los requisitos de retención específicos de la industria.
- Auditorías de revisión de acceso: Realiza auditorías de acceso periódicas para garantizar que sólo las personas autorizadas tengan acceso a áreas confidenciales.
- Manejo seguro de datos de usuario: Sigue las mejores prácticas para almacenar y procesar datos personales relacionados con el control de acceso.

Gestión de identidades y credenciales

- Adopta la autenticación de múltiples factores: Combina tarjetas RFID con biometría (huella dactilar, reconocimiento facial) o autenticación móvil para una mayor seguridad.
- Utiliza credenciales inteligentes: Implementa tarjetas inteligentes encriptadas, credenciales basadas en dispositivos móviles o gestión de identidad basada en blockchain.
- Automatiza la revocación de acceso: Integra la TSO con los sistemas de RR.HH. para revocar automáticamente el acceso cuando el empleado se va.
- Autenticación biométrica: Implementa sistemas de acceso biométrico en áreas de alta seguridad para eliminar los riesgos de tarjetas perdidas o clonadas.

Ciberseguridad

- Cifrado de extremo a extremo: Asegúrate de que todos los datos de la TSO, incluidas las credenciales y los registros, estén encriptados (se recomienda la encriptación AES-256 o superior).
- MFA: Utiliza MFA para interfaces de gestión de la TSO y funciones de seguridad críticas.
- Aplicación periódica de parches y actualizaciones de firmware: Mantén todos los dispositivos de la TSO actualizados con parches de seguridad para cerrar vulnerabilidades.
- Segmentación de red: Aísla la TSO de las redes de TI generales para evitar el movimiento lateral en caso de un ciberataque.
- Pruebas de penetración y auditorías de seguridad: Prueba periódicamente la TSO para detectar vulnerabilidades y realiza auditorías de seguridad de terceros.

Rendimiento

- TSO basada en la nube y SaaS: Implementa

una TSO basada en la nube donde tenga sentido lograr una escalabilidad perfecta en múltiples ubicaciones.

- Equilibrio de carga y redundancia: Implementa arquitecturas de servidores escalables con redundancia para manejar el aumento de la demanda.
- Computación en el borde: Utiliza controladores de borde inteligentes para procesar decisiones de control de acceso localmente y reducir la dependencia de los servidores centrales.
- RBAC: Implementa permisos jerárquicos para simplificar la gestión a medida que el sistema escala.

Capacitación

- Interfaces fáciles de usar: Elige soluciones de TSO con interfaces de usuario intuitivas para reducir la complejidad de la capacitación.
- Programas de concientización sobre la seguridad: Lleva a cabo sesiones de capacitación continua para empleados sobre las mejores prácticas para el control de acceso.
- Gestión de acceso móvil y remoto: Ofrece soluciones de acceso basadas en dispositivos móviles para una autenticación cómoda y segura.
- Gamificación e incentivos: Utiliza programas de capacitación en seguridad con recompensas para fomentar el cumplimiento y la concientización.

Pensamiento a gran escala: Diseño de una estrategia conectada a los sistemas de la TSO

Identifica los activos

Identificar los activos importantes que requieren seguridad es la primera etapa para la protección de una organización. Por lo general, estos recursos consisten en sistemas de tecnología operativa, empleados, datos confidenciales e infraestructura física. Los equipos de seguridad pueden gestionar efectivamente los recursos y priorizar las actividades de protección cuando tienen una comprensión clara de lo que es valioso dentro de una organización. Las organizaciones pueden comenzar a sentar las bases de su estrategia de seguridad y garantizar que los recursos más preciados estén protegidos al máximo nivel identificando todos sus activos operativos importantes. Este paso también implica determinar las dependencias, clasificar los activos según su importancia y comprender cómo las amenazas a la seguridad podrían afectar la continuidad operativa.

Evalúa el riesgo

Las organizaciones deben utilizar evaluaciones de riesgos y auditorías de seguridad para analizar posibles amenazas y vulnerabilidades una vez identificados los activos. Esto implica examinar los riesgos internos, incluidas las amenazas internas, las políticas y el cumplimiento normativo, y las fallas estructurales. Además, las organizaciones deben identificar amenazas externas, como invasiones, ciberataques y robos. Las organizaciones pueden centrar sus planes de seguridad utilizando la información de una evaluación de riesgos integral basada en la gravedad de diversas vulnerabilidades de seguridad. Las organizaciones pueden anticiparse a las amenazas en desarrollo y modificar sus medidas de seguridad en consecuencia realizando evaluaciones de riesgos de forma periódica, según lo consideren necesario. Esto garantiza que las vulnerabilidades se identifiquen, se solucionen y se prueben antes de que los actores de amenazas las exploten.

Controla el acceso

Una medida de seguridad fundamental es el control de acceso. El control de acceso garantiza que sólo las personas con permiso puedan interactuar con ubicaciones, activos operativos o datos confidenciales. Las organizaciones deben implementar medidas de seguridad como sistemas de gestión de visitantes, escáneres biométricos, tarjetas de acceso, autenticación de múltiples factores y controles de acceso basados en roles. Estas precauciones reducen la posibilidad de amenazas internas, violaciones físicas y accesos ilegales. Un control de acceso efectivo no sólo protege zonas privadas sino que también permite que los controles de seguridad monitoreen los movimientos y actividades de las personas dentro de las instalaciones de una organización. Las organizaciones pueden identificar irregularidades y regulaciones de seguridad con la ayuda de auditorías de rutina y monitoreo de registros de acceso.

Monitorea las actividades

Los sistemas de seguridad se monitorean continuamente para garantizar que se identifiquen todas las actividades sospechosas y se resuelvan rápidamente antes de que se salgan de control. Para proporcionar un monitoreo continuo de las instalaciones, las organizaciones deben implementar tecnologías de detección de intrusos, detectores de movimiento, sistemas de alarma y cámaras CCTV. Las regiones confidenciales, como las zonas de alto riesgo, las áreas sensibles y los puntos de acceso, deben estar bajo vigilancia constante. Las organizaciones pueden mejorar rápidamente la eficiencia de sus medidas de seguridad al combinar la vigilancia automatizada con la supervisión humana en tiempo real.

Asegura el perímetro

La primera línea de defensa contra ataques y accesos ilegales de amenazas externas es un perímetro bien seguro y definido. Para prevenir y redirigir incursiones no deseadas, las organizaciones deben contar con barreras físicas robustas que incluyan puntos de control de seguridad, puertas reforzadas, cercas y puntos de entrada controlados. Proteger el acceso de peatones y vehículos es otro aspecto de una seguridad perimetral efectivo, que garantice que sólo personas con permiso puedan entrar en cualquier lugar cercano a áreas restringidas. Crear una atmósfera de seguridad disuadirá las amenazas externas no deseadas. Mejorar la seguridad del perímetro minimizando los puntos ciegos y disuadiendo a los intrusos se puede lograr mediante iluminación, señalización y diseño ambiental. Además de proteger los activos, un perímetro seguro agrega otra línea de defensa que complementa los protocolos de seguridad internos.

Desarrolla respuestas

Las organizaciones están mejor equipadas para responder con rapidez y eficiencia en caso de emergencias, desastres o violaciones de seguridad cuando cuentan con una estrategia clara de respuestas. En los planes de respuesta a incidentes deben describirse procedimientos específicos para abordar diversos riesgos, incluidas incursiones físicas, ciberataques, catástrofes naturales y ataques internos. Los planes de respuesta a incidentes deben abarcar todas las tareas asignadas al personal para extinguir todas y cada una de las amenazas. Para garantizar el éxito de un plan de respuesta, las organizaciones deben establecer procedimientos de comunicación claros, asignar equipos de respuesta y realizar simulacros de emergencia frecuentes a nivel interno. Asegurarse de que los empleados estén bien informados durante una emergencia es crucial para la seguridad de los empleados de una organización. Una estrategia de respuesta efectiva reduce los efectos de los eventos de seguridad, protege a los empleados y la propiedad y garantiza que las interrupciones se gestionen de manera eficaz. Las organizaciones pueden mejorar su capacidad para manejar incidentes de seguridad y recuperarse rápidamente de posibles amenazas revisando y poniendo a prueba de forma periódica sus planes de respuesta.

Capacita a tu personal

La efectividad de la respuesta de seguridad depende de las personas encargadas de llevarla a cabo. Una capacitación frecuente sobre concientización ayudará a los miembros del personal y a los equipos de seguridad a comprender sus responsabilidades para preservar la seguridad de su lugar de trabajo. Los trabajadores deben recibir capacitación sobre las mejores prácticas de ciberseguridad, protocolos de emergencia, pautas de control de acceso y otras medidas de seguridad que protejan mejor los activos de la organización. Con el fin de estar listos para enfrentar las amenazas del mundo real, los equipos de seguridad deben participar en capacitaciones basadas en escenarios. La capacitación repetitiva refuerza los deberes y las expectativas de los empleados que gestionan el resultado de los eventos de seguridad. La eficacia de la seguridad de una organización aumenta y las posibilidades de error se reducen enormemente cuando existe una cultura de conciencia de seguridad que rodea a la organización.

Construye para adaptarte a las necesidades de tu organización

Existen innumerables recursos que asesoran a las empresas sobre sus necesidades. Las TSO sólo son beneficiosos operativamente si se adaptan a las necesidades operativas específicas de una organización o negocio. Un restaurante de comida rápida no necesita una bóveda bancaria, sino probablemente necesite una caja de seguridad para las transacciones diarias. Esto no quiere decir que una bóveda de banco no proteja los artículos que contiene, pero sería poco práctica, costosa e innecesaria para las operaciones diarias del restaurante. Encontrar lo que se adapte a las necesidades de una empresa no tiene por qué ser una tarea difícil. La clave es evaluar los riesgos asociados a las necesidades operativas, priorizar uno de ellos y seleccionar tecnologías que optimicen eficientemente la seguridad en toda la organización. Tras identificar los objetivos de seguridad de una organización, debes decidir qué tecnologías se adaptan mejor a cada objetivo. Por ejemplo, un sistema de vigilancia no tiene como objetivo detener o alertar a visitantes no autorizados que entren a un establecimiento, pero un sistema de control de acceso físico sí lo tiene. Quizás necesites ambos, quizás no. Construye a tu medida.

La escalabilidad es la clave

La escalabilidad en la implementación de una TSO es crucial para mantener soluciones de seguridad a largo plazo. Si el objetivo de la organización es el crecimiento operativo, la postura de seguridad física también debe poder crecer. Al agregar tecnologías modulares, automatizadas y compatibles, las organizaciones tendrán la capacidad de hacer crecer su postura de seguridad física en paralelo al crecimiento de sus operaciones y necesidades relacionadas. Por ejemplo, una PYME con una o dos ubicaciones puede necesitar sólo una pequeña inversión en una TSO, pero a medida que esta organización se modernice o se expanda a otras lugares, puede requerir una inversión mayor. Priorizar la escalabilidad permite proteger los activos, reducir los costos y las complejidades a largo plazo de las actualizaciones de una TSO.

Primero la funcionalidad

Cuando se trata de una TSO, la funcionalidad es lo primero. "La clave es que la función se esté realizando. Cómo se la realiza es secundario y depende completamente de la organización y sus requisitos únicos."[31] La seguridad no es una solución única para todos. La implementación de una TSO mínima pero funcional puede ser un factor disuasorio suficiente para muchas organizaciones. Por ejemplo, una pequeña empresa o una empresa nueva podrían tener restricciones de presupuestos con respecto a la seguridad. Sin un presupuesto para un equipo de seguridad designado o sistemas complejos, esa organización puede estar justificada en abordar su seguridad física con un sistema de vigilancia simple, alarmas y puertas cerradas. La inclinación del espectro de seguridad de lo simple hacia lo complejo debería ocurrir una vez que una evaluación de riesgos exhaustiva justifique la necesidad de medidas avanzadas. Esta idea parece devolvernos a nuestro concepto original y vincula el círculo al edificio para que se adapte a tus necesidades.

31 Protegiendo tu sistema: Seguridad física. Visto el 29 de enero de 2025. [Online]. Disponible en inglés: https://nces.ed.gov/pubs98/safe-tech/chapter5.asp

APÉNDICE C

Puntos destacados

1) La TO tiende a existir en puntos de convergencia y a menudo se intersecta con una variedad de necesidades, requisitos y funciones utilitarias. Y en estas intersecciones, el contexto, el propósito y los detalles a menudo variarán. Por lo tanto, la interpretación humana estará influenciada por una diversidad de experiencias separadas y puntos de vista resultantes. Todos proporcionan valor.
2) Las TSO son los elementos técnicos subyacentes que nos permiten hacer nuestro trabajo como profesionales de la seguridad; tecnologías utilizadas para ayudarnos a respaldar, automatizar, escalar y entregar la misión principal de la seguridad física; la TSO ayuda a gestionar los problemas de seguridad y nos conecta con el mundo físico que intentamos proteger.
3) Comprender, como profesionales de la seguridad, algunos de los principios y desafíos relacionados con los tipos de TSO de los que dependemos a diario puede marcar una diferencia significativa cuando nos enfrentamos a una complejidad creciente y a amenazas en evolución. Junto con las expectativas de cero fallos y al mismo tiempo garantizando resultados críticos para la misión, la TSO es significativamente importante para la industria de la seguridad.
4) Las soluciones de TSO complejas pueden brindar muchos beneficios, pero no siempre son fáciles de implementar y mantener. La implementación, la integración y el mantenimiento continuo del ciclo de vida no son tan simples en muchos casos y deben planificarse y manejarse con cuidado. Ten un plan
5) El dominio de las TSO es una red compleja de desafíos y dificultades, pero ninguno es insuperable y los resultados de seguridad al final del recorrido bien valen las inversiones necesarias. Proteger a las personas, la propiedad y los recursos valiosos es un objetivo noble. Pero no es sencillo. Al trabajar juntos y compartir nuestras valiosas experiencias y conocimientos del dominio, podemos garantizar el éxito mutuo mediante la elaboración de estrategias colaborativas y la resolución de los desafíos para garantizar mejor la entrega óptima y las mejores prácticas operativas.

Referencias

1. Tendencias del mercado de la tecnología operativa. Visto el: 26 de octubre de 2024. [Online]. Disponible en inglés: https://www.grandviewresearch.com/industry-analysis/operational-technology-market-report (Grand View Research, 2024)
2. Tamaño y pronóstico del mercado de la tecnología operativa. Visto el: 26 de octubre de 2024. [Online]. Disponible en inglés: https://www.verifiedmarketresearch.com/product/operational-technology-market (Verified Market Research, 2024)
3. 7 pasos para alinear a TI, TO y seguridad física. Visto el: 26 de octubre de 2024. [Online]. Disponible en inglés: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/11/29/7-steps-to-align-it-ot-and-physical-security. (IANS 2022)
4. ¿En qué se diferencian la TO y la TI? Visto el: 27 de octubre de 2024. [Online]. Disponible en inglés: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html (Cisco)
5. Tecnología operativa (TO) Visto el: 27 de octubre de 2024. [Online]. Disponible en inglés: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot (Gartner)
6. ¿Qué es la tecnología operacional? Visto el: 27 de octubre de 2024. [Online]. Disponible en inglés: https://www.redhat.com/en/topics/edge-computing/what-is-ot (Red Hat, 2022)
7. Control de acceso físico: Encuesta revela nuevas tendencias de implementación, L. Merredew. Visto el: 2 de noviembre de 2024. [Online]. Disponible en inglés: https://www.securitymagazine.com/articles/98710-physical-access-control-survey-reveals-new-deployment-trends. (Security Magazine, 2022)
8. Cómo la automatización obsoleta conduce a un mayor esfuerzo manual y qué puedes hacer al respecto, N. Kinson. Visto el: 3 de noviembre de 2024. [Online]. Disponible en inglés: https://www.redwood.com/article/how-outdated-automation-leads-to-more-manual-effort-and-what-you-can-do-about-it (Redwood, 2022)
9. Por qué los empleados con exceso de trabajo son un riesgo para la seguridad, D. Kelley. Visto el: 3 de noviembre de 2024. [Online]. Disponible en inglés: https://securityintelligence.com/security-risk-staffing-it-teams-overworked-employees (Security Intelligence, 2014)
10. Interoperabilidad de sistemas de seguridad y protección, Pkimluker. Visto el: 9 de noviembre de 2024. [Online]. Disponible en inglés: https://www.clr2wrk.com/safety-and-security-systems-interoperability (Clear 2 Work, 2022)
11. Sistemas de control de acceso físico 101. Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://www.idmanagement.gov/university/pacs/ (Oidmanagement.gov, 2023)
12. 10 tipos de sistemas de control de acceso físico, OLOID Desk. Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://www.oloid.ai/blog/10-types-of-physical-access-control-system (Oloid, 2023)
13. Integración de IAM con sistemas de control de acceso físico, D. Simmons. Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://techvisionresearch.com/wp-content/uploads/2020/03/PACS-LACS-20200310-excerpt-final.pd (TechVision Research, 2020)
14. Perspectiva tecnológica para sistemas de control de acceso físico. Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://www.gartner.com/en/documents/3451120 (Gartner, 2016)
15. Drones domésticos. Visto el: 22 de enero de 2025. [Online]. Disponible en inglés: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones (ACLU, 2025)
16. Diseño de sistemas de monitoreo de seguridad física para vigilancia y respuesta a la calidad del agua. Visto el 24 de enero de 2025. [Online]. Disponible en inglés: https://www.epa.gov/sites/default/files/2017-11/documents/esm_design_guidance_2017-11-02.pdf (EPA, 2017)
17. 7 componentes ambientales a tener en cuenta durante una auditoría de seguridad física. Visto el 25 de enero de 2025. [Online]. Disponible en inglés: https://www.security101.com/blog/7-environmental-components-to-take-in-consideration-during-a-physical-security-audit (Security 101, 2025)
18. Falsas alarmas de incendio. Visto el 27 de enero de 2025. [Online]. Disponible en inglés: https://www.firehouse.com/home/news/10545242/false-fire-alarms (Firehouse, 1996)
19. 3 consejos para ayudar a reducir el riesgo de falsas alarmas. Visto el 27 de enero de 2025. [Online]. Disponible en inglés: https://www.adtsecurity.com.au/blog/security-tips-community/risk-of-false-alarms (ADT, 2025)
20. 7 formas de prevenir falsas alarmas en tu sistema de seguridad. Visto el 27 de enero de 2025. [Online]. Disponible en inglés: https://adssecurity.com/prevent-false-alarms-with-your-security-system (Vector Security, 2021)
21. ¿Qué es un sistema de gestión de edificios? Visto el 10 de febrero de 2025. [Online]. Disponible en inglés: https://www.cim.io/blog/what-is-a-building-management-system (CIM, 2025)
22. Cómo la integración de sistemas de seguridad con un BMS puede ayudar a mejorar la seguridad de la propiedad comercial. Visto el 10 de febrero de 2025. [Online]. Disponible en inglés: https://stealthmonitoring.com/crime-prevention/how-integrating-security-systems-with-bms-can-help-elevate-commercial-property-security (Stealth Monitoring, 2025)
23. El desafío de proteger los sistemas de gestión de edificios, E. Ben-Meir. Visto el 3 de febrero de 2025. [Online]. Disponible en inglés: https://www.techtarget.com/iotagenda/blog/IoT-Agenda/The-Challenge-Of-Securing-Building-Management-Systems (TechTarget, 2019)
24. Iluminando el camino hacia una ciudad más inteligente y segura. Visto el 31 de enero de 2025. [Online]. Disponible en inglés: https://www.securityindustry.org/2018/09/14/lighting-the-way-to-a-smarter-safer-city/ (SIA, 2018)
25. El mejor software de seguridad física. Visto el 1 de febrero de 2025. [Online]. Disponible en inglés: https://www.softwareworld.co/physical-security-software/ (SoftwareWorld, 2025)
26. Los beneficios de la integración de la seguridad contra incendios, la protección de la vida y la seguridad, T. Giannini. Visto el 4 de febrero de 2025. [Online]. Disponible en inglés: https://www.buildings.com/industry-news/article/10189775/the-benefits-of-fire-life-safety-and-security-integration (Buildings, 2012)
27. Encuesta de PwC sobre tendencias digitales en operaciones en 2024: Por qué aún es difícil lograr resultados comerciales significativos y qué puedes hacer. Visto el: 9 de noviembre de 2024. [Online]. Disponible en inglés: https://www.pwc.com/us/en/services/consulting/business-transformation/digital-supply-chain-survey.html (PwC, 2024)
28. El riesgo es dinámico, por lo que la evaluación del riesgo físico debe ser continua, D. Young, M. Martin. Visto el: 1 de diciembre de 2024. [Online]. Disponible en inglés: https://www.asisonline.org/security-management-magazine/articles/2023/11/dynamic-risk-assessment/continuous-physical-risk-assessment (ASIS, 2023)
29. Los 15 mayores riesgos de la inteligencia artificial, B. Marr. Visto el: 1 de diciembre de 2024. [Online]. Disponible en inglés: https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence (Forbes, 2023)
30. 8 desafíos que enfrenta todo centro de operaciones de seguridad, J. Burke. Visto el: 1 de diciembre de 2024. [Online]. Disponible en inglés: https://www.techtarget.com/searchsecurity/tip/8-challenges-every-security-operations-center-faces (Tech Target, 2020)

**PRODUCIDO CON EL GEN-
EROSO APOYO DE**

securityindustry.org