SECURITY INDUSTRY ASSOCIATION

SEGURIDAD EN CENTROS DE DATOS

Guía de tendencias y estrategias para la seguridad física de las instalaciones de centros de datos

PRODUCIDO CON EL APOYO DE

MOTOROLA SOLUTIONS

PAVION CONNECT AND PROTECT

PLUGOUT

Precio del informe

USD$99

Si eres empleado de una empresa miembro de SIA, puedes descargar este informe de forma gratuita gracias a la membresía de tu empresa.

Contenido

Autor

Amy Dunton, Co-Presidente
Subcomité de seguridad perimetral de SIA y socio director de Sulton Security

©2025 Security Industry Association.
Todos los derechos reservados.

Resumen

El mercado mundial de centros de datos está creciendo a un ritmo sin precedentes. En 2025, el mundo generará 181 zettabytes de datos, lo que supone un aumento del 23% con respecto al año anterior. Esto se traduce en 2,5 trillones de bytes creados cada día: 29 terabytes por segundo. Esta demanda explosiva de almacenamiento y procesamiento lleva a que la industria se concentre en la energía y la refrigeración. Sin embargo, mientras esas conversaciones acaparan la atención, la seguridad física queda en un segundo plano, a pesar de ser igualmente fundamental para la resiliencia. Al mismo tiempo, el aumento de la demanda está transformando el mercado con un crecimiento a gran escala, competencia en el sector de data centers compartidos y expansión empresarial.

El rápido crecimiento trae consigo nuevas complejidades: especificaciones obsoletas, sistemas de seguridad aislados y socios con experiencia en otros mercados pero que no están familiarizados con las exigencias específicas de los centros de datos, todo lo cual amenaza la resiliencia de la infraestructura digital crítica. Este informe examina los desafíos que configuran la seguridad física de los centros de datos en la actualidad, centrándose en la integración, la interoperabilidad y la gestión del ciclo de vida. A partir de la experiencia de fabricantes, integradores y usuarios finales, este informe destaca no sólo las tecnologías emergentes, sino también los riesgos persistentes de considerar la seguridad como algo secundario. El resultado es una hoja de ruta con visión de futuro para ofrecer una seguridad sólida que impulse el crecimiento, en lugar de obstaculizarlo.

PRODUCIDO CON EL APOYO DE

MOTOROLA SOLUTIONS

PAVION CONNECT AND PROTECT

PLUGOUT

Introducción: El dinámico panorama de riesgos

A pesar de décadas de incidentes y miles de millones invertidos en ciberseguridad, la protección física en muchos centros de datos siguen limitándose a sólo el 5% o menos del presupuesto total de construcción, y a veces incluso a menos del 1% en el caso de las grandes empresas de centros de datos que construyen a gran escala. Con bastante frecuencia, las medidas de seguridad física se eliminan en las últimas fases de la optimización de costos, se copian de especificaciones obsoletas o se implementan sin tener en cuenta la integración entre el perímetro, el control de acceso y la vigilancia.[1]

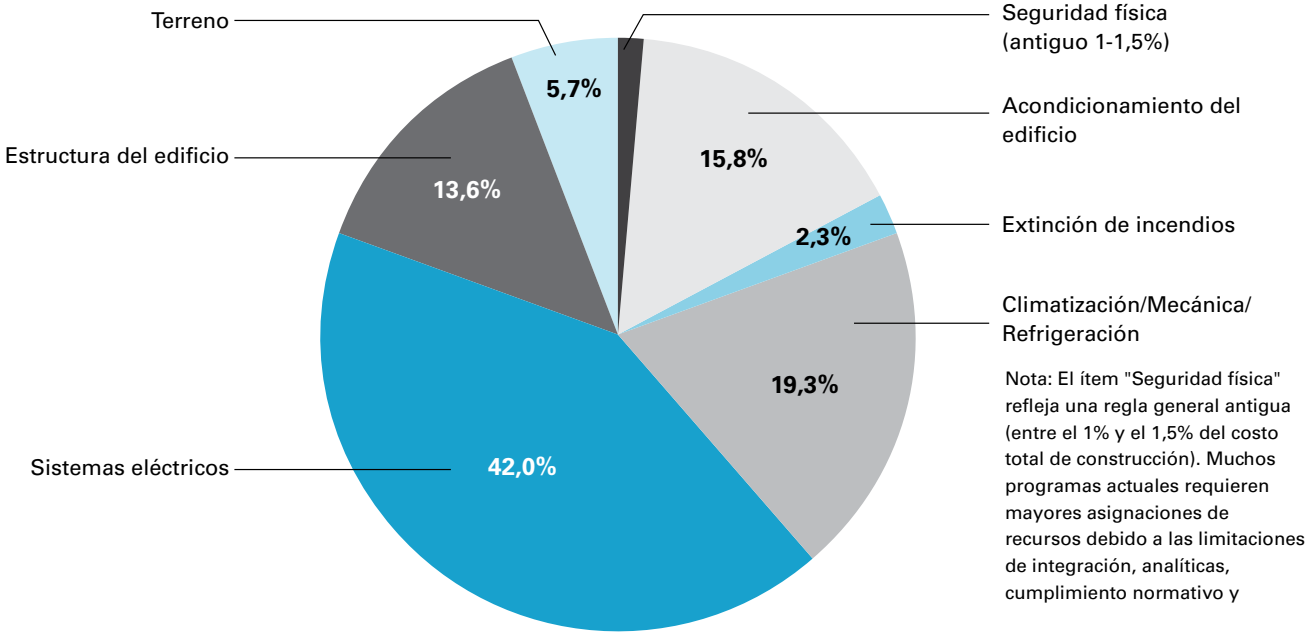
Los resultados son predecibles: rediseños costosos, puntos ciegos operativos y mayor responsabilidad.

Las presiones para acelerar la comercialización agravan estos problemas. Actualmente, campus completos se construyen en fases de construcción superpuestas; los operadores ponen en funcionamiento un edificio o una sala de datos mientras que las áreas adyacentes siguen siendo zonas de trabajo activas. Esto eleva el riesgo: los racks con equipos en funcionamiento y la actividad del personal de seguridad se encuentran junto a obras de construcción pesada, lo que genera problemas de seguridad, acceso y respuesta ante incidentes. Los integradores deben realizar las puestas en marcha en cuestión de días en lugar de semanas, con poca tolerancia a los errores.

Finalmente, el ritmo y la magnitud del proyecto han atraído a una gran cantidad de socios experimentados de otros sectores: arquitectos, ingenieros, contratistas generales, subcontratistas e integradores que destacan en otros ámbitos, pero que quizás sean nuevos en las normas de los centros de datos. Sin la formación adecuada y los requisitos comunes, las suposiciones propias del sector del retail o del almacenamiento se trasladan a entornos con requisitos de disponibilidad, cumplimiento normativo y usuarios sustancialmente diferentes.

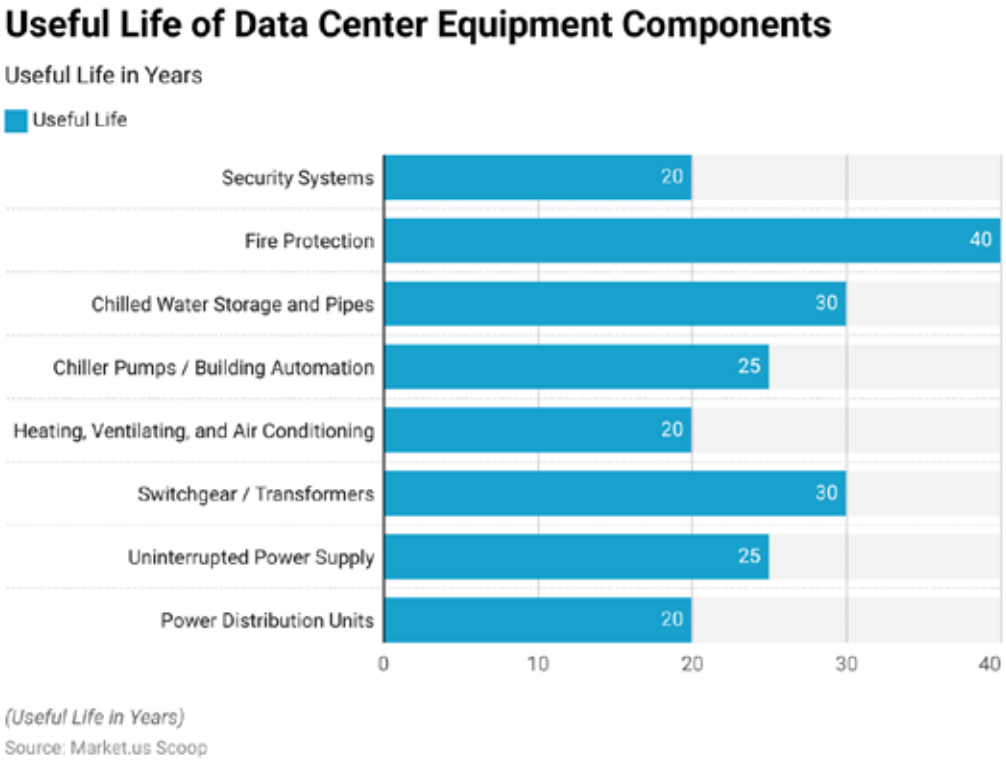
Este documento técnico no es una simple lista de verificación. Consolida las perspectivas de operadores, integradores y fabricantes para exponer las deficiencias sistémicas y destacar cómo la innovación está cambiando la situación, desde las analíticas con inteligencia artificial (IA) que reducen drásticamente las alarmas innecesarias, hasta los modelos de gobernanza que elevan la seguridad a las primeras fases de las decisiones de diseño.

Asignación ilustrativa de presupuesto para la construcción de un centro de datos
(Separando lo antiguo 1-1,5% del ítem 'Seguridad Física')



Nota: El ítem "Seguridad física" refleja una regla general antigua (entre el 1% y el 1,5% del costo total de construcción). Muchos programas actuales requieren mayores asignaciones de recursos debido a las limitaciones de integración, analíticas, cumplimiento normativo y

1. En este estudio, el término "vigilancia" se refiere en términos generales a las funciones de monitoreo, que pueden incluir, entre otras cosas, sistemas de videovigilancia (por ejemplo, cámaras, analíticas de video y sensores de apoyo).



Estado actual de la seguridad física de los centros de datos

Históricamente, la seguridad física ha recibido menos atención y financiación que la infraestructura de energía, refrigeración y redes. Con presupuestos que rondan el 5% del costo total de la construcción, la seguridad suele ser el primer ítem que sufre recortes ante la presión económica. Esos recortes rara vez desaparecen; al contrario, reaparecen en forma de modificaciones posteriores y problemas operativos. Sin embargo, recortar la seguridad a menudo puede conllevar riesgos de auditoría y cumplimiento normativo, por lo que los presupuestos de seguridad de los centros de datos no se recortan con tanta frecuencia como en otros sectores.

A menudo se adoptan especificaciones de otras industrias o de generaciones anteriores de centros de datos. En la práctica, esto genera fallos predecibles: cámaras montadas a 18 pies de altura que se espera que realicen reconocimiento facial, reconocimiento de placas vehiculares especificado en ángulos que son ópticamente imposibles y lectores de control de acceso que obligan a los edificios con múltiples usuarios a desplegar "granjas de lectores" porque no pueden interoperar entre sí. Los operadores informan que, una vez finalizada la garantía, descubren que faltan componentes clave de la solución o que están instalados de forma incorrecta, con pocas posibilidades de recuperar los costos.

A menudo se adoptan especificaciones de otras industrias o de generaciones anteriores de centros de datos. En la práctica, esto produce fallos predecibles, como:

- Cámaras instaladas a 18 pies de altura, pero que se espera que proporcionen reconocimiento facial
- Reconocimiento de placas vehiculares especificadas en ángulos que son ópticamente imposibles
- Lectores de control de acceso que obligan a los sitios con múltiples usuarios a implementar "granjas de lectores" porque no pueden interoperar entre sí
- Instalaciones preliminares y ubicaciones de los equipos de cabecera colocados incorrectamente, lo que requiere costosos trabajos de rectificación
- Sistemas de seguridad perimetral que no están operativos antes de que el centro de datos entre en funcionamiento, lo que obliga a los propietarios a recurrir a medidas temporales hasta que se solucionen los problemas
- Una vez finalizada la garantía, se descubre que faltan componentes clave de la solución o que están instalados incorrectamente, con pocas posibilidades de recuperar los costos

La seguridad suele representar apenas un porcentaje mínimo de los presupuestos de construcción, lo que la convierte en el primer lugar

La responsabilidad en el diseño está fragmentada. Los elementos perimetrales (por ejemplo, vallas, puertas, bolardos) suelen incluirse dentro de las divisiones de construcción, mientras que el control de acceso, el video, la gestión de visitantes y las alarmas quedan bajo el departamento de seguridad. Sin un responsable de la integración, los sistemas funcionan en silos. Incluso cuando existen especificaciones detalladas, a menudo de más de 70 páginas con números de modelo y de pieza exactos, la visibilidad sobre lo que realmente piden los subcontratistas puede ser limitada; las sustituciones pasan desapercibidas hasta que se produce un fallo.

La escala global añade complejidad. Los profesionales del sector afirman que una cobertura de integración verdaderamente "global" es poco común. Ni siquiera se logra una coherencia a nivel nacional. La respuesta pragmática, señalan muchos operadores, es contar con una lista de múltiples integradores, a menudo cinco o más, que se ajusten a estándares y normas de gobernanza comunes, en lugar de un modelo de proveedor único que no puede seguir el ritmo de la velocidad y la expansión geográfica.

Tendencias del mercado y tecnología que están perfilando el futuro

La inteligencia artificial y las analíticas avanzadas están redefiniendo las expectativas. Los usuarios finales informan que las analíticas basadas en inteligencia artificial puede reducir las alarmas innecesarias hasta en un 90%, alcanzando una alta precisión tras un breve período de aprendizaje. A medida que las analíticas maduran, van más allá de la detección para centrarse en la clasificación, diferenciando la actividad inofensiva de las amenazas creíbles y notificando a los operadores sólo sobre los eventos que requieren acción.

La integración se está ampliando de "video + acceso" hasta incluir radios/voz, sistemas de detección de intrusiones, radares, cámaras térmicas y sensores ambientales. El resultado no es simplemente alertas por sí solas, sino respuestas coordinadas: acciones basadas en políticas que activan puertas, cámaras y sistemas de comunicación de forma conjunta. Igualmente, el control de versiones es importante: las bases de software incompatibles suelen provocar fallos en integraciones que, de otro modo, funcionarían correctamente.

La gestión de adquisiciones está evolucionando. Los modelos "como servicio" transforman los gastos de capital en gastos operativos, incorporan ciclos de actualización y ayudan a los operadores a evitar la dependencia de plataformas obsoletas. Las especificaciones basadas en el rendimiento están sustituyendo a las especificaciones definidas por los fabricantes, lo que abre la puerta a los innovadores, siempre y cuando puedan cumplir con los requisitos de escala e interoperabilidad.

Las exigencias en materia de sostenibilidad (eficiencia energética, menor dependencia del personal de seguridad, implementaciones modulares) conforman hoy las estrategias de seguridad física. Uno de los principales motivos para adoptar tecnologías emergentes es reducir la dependencia de los

No hay que confundir cumplir con las especificaciones de rendimiento con satisfacer la necesidad.
Una puerta cumple con la clasificación de resistencia a impactos, pero no se puede supervisar desde la central; un lector cumple con el alcance, pero carece de controladores compatibles; las cámaras cumplen con la resolución, pero no se integran con el sistema de gestión de video; los sensores emiten alarmas, pero los eventos no se pueden transmitir al sistema de gestión de información y eventos de seguridad. Especificar los resultados y la integración para que "cumpla con la normativa" significa también que

Los usuarios finales informan que las analíticas basadas en inteligencia artificial pueden reducir las alarmas innecesarias hasta en un 90%,

guardas de seguridad presenciales: los operadores priorizan las capacidades que sustituyen los puestos fijos por sistemas de detección automatizada y verificable y respuesta remota (video con analíticas, fusión de sensores, intercomunicadores inteligentes, robótica y centros de operaciones de seguridad globales gestionados), preservando o mejorando la detección y la respuesta, al tiempo que se destinan las horas de trabajo de los guardas a tareas de mayor valor. La globalización plantea una última tendencia: pocos socios pueden garantizar realmente una implementación coherente en todas las regiones. Muchos operadores prefieren enfoques híbridos: estándares y gobernanza globales combinados con una sólida ejecución local, para poder lograr coherencia sin sacrificar la agilidad regional.

Consideraciones estratégicas para fabricantes e integradores

Empiecen por el mercado, no por el producto.

El sector de los centros de datos no es un ámbito en el que se puedan copiar y pegar los enfoques utilizados en las empresas, el retail, la educación o el almacenamiento. Eso puede ser como enfrentar una batalla de ciberseguridad con un cuchillo de madera. El tiempo de actividad, la rapidez de comercialización, la complejidad de la arquitectura multiusuario, la disciplina con las versiones y los patrones de entrega globales y locales hacen que este entorno sea fundamentalmente diferente. Los fabricantes e integradores que tienen éxito aquí comienzan por comprender el modelo operativo en el que se adentran: cómo se desarrollan las diferentes fases de los campus, cómo se rigen las normas, cómo los usuarios determinan los requisitos y cómo se distribuye la responsabilidad desde el diseño hasta la puesta en marcha y las operaciones.

Si tu estrategia comienza con "qué vendemos" en lugar de "cómo se construyen y gestionan los centros de datos",

Lo que "comprender el mercado" significa en la práctica

- **Realidades sobre el tiempo de actividad y las fases de implementación:** Las construcciones en tiempo real (la "parte 1.1" está disponible en línea mientras que las áreas adyacentes aún están en construcción) modifican los métodos de gestión de riesgos, secuenciación y puesta en marcha.
- **Matices entre entornos multiusuario y de data centers compartidos:** Los estándares para lectores, los modelos de credenciales y los flujos de trabajo para visitantes deben coexistir sin necesidad de "granjas de lectores" y sin depender de sistemas propietarios.
- **Estándares globales, ejecución local:** Prevén un modelo de implementación híbrido: estándares y gobernanza centrales, ejecutados por múltiples integradores regionales.
- **El control de versiones como disciplina:** Las pequeñas discrepancias en el firmware o el software suelen provocar fallos en las integraciones— planificar pruebas de referencia y de regresión.
- **Gobernanza y aceptación:** Las especificaciones basadas en el rendimiento, las pruebas de verificación y los resultados medibles son cada vez más normales.

Recursos adicionales

El reciente simposio Vertical Insight sobre centros de datos de SIA ofrece información y estrategias de mercado de Allegion, SAGE Integration y Wesco, y está disponible como grabación por demanda.

ALLEGION SAGE integration wesco

La interoperabilidad no es negociable.

Los operadores esperan sistemas **API-first** que se integren con sistemas de seguridad perimetral, control de acceso, video, voz, detección de intrusión, radar/sensores térmicos y sensores ambientales. Los productos que no puedan participar en un ecosistema más amplio quedarán relegados, independientemente de la cantidad de funciones que ofrezcan.

Demuestren que pueden cumplir con los objetivos a gran escala.

Los nuevos participantes suelen subestimar lo siguiente: los productos deben ser capaces de superar las pruebas de seguridad de las aplicaciones, la revisión de las unidades de mantenimiento de existencias (SKU) a nivel global, la logística, las piezas de repuesto y las autorizaciones de devolución de materiales (RMA), así como el equipo de ingeniería de campo necesario para una respuesta las 24 horas del día, los 7 días de la semana. Los compromisos deben estar a la altura de la capacidad: prometer demasiado a gran escala erosiona rápidamente la confianza y es difícil recuperarla.

Estructuren sus organizaciones para el ámbito vertical.

Los centros de datos no se ajustan perfectamente a las jerarquías de ventas regionales. Equipos ganadores:

- Designen **"capitanes" globales de cuentas** con autoridad sobre los estándares y las métricas de éxito
- Utilicen **equipos de entrega regionales** para la ejecución y el mantenimiento en el lugar
- Alineen la **remuneración con los resultados obtenidos** con los clientes, no con las victorias territoriales (para evitar la fricción interna que percibe el cliente)

Compitan en función del ciclo de vida del producto, no de las partidas individuales

Consideren los programas como **asociaciones a largo plazo**. Prevean revisiones de proveedores, proyectos piloto y pruebas de integración que duren entre 6 y 12 meses o más antes de su inclusión estándar. Elaboren ofertas que incluyan la actualización del ciclo de vida, comprobaciones de estado, gestión de versiones y rutas de actualización, y no sólo la instalación inicial.

Tengan cuidado con las trampas de la ingeniería de valor.

Las especificaciones basadas en el rendimiento son útiles, pero sólo si se controlan las sustituciones. Las "alternativas de bajo costo" que comprometen la interoperabilidad o la durabilidad generan riesgos para los usuarios y los operadores, y suponen mayores costos en reformas y daños a la reputación.

LISTA DE

¿Estás preparado para el mercado de los centros de datos?

- [ ] ¿Hemos mapeado nuestros **puntos de integración**(APIs, eventos, identidad, voz) con el ecosistema del operador?
- [ ] ¿Podemos mantener **todos los sitios alineados** en la misma versión y demostrar, mediante pruebas, que **las actualizaciones no dañarán las funciones existentes**, al ritmo que exigen los operadores?
- [ ] ¿Contamos con **SKU/logística a nivel global** y un plan realista de **RMA/ respuesta sobre el terreno**?
- [ ] ¿Está nuestro equipo **organizado en función de las cuentas**, con un departamento especializado en centros de datos y una clara transferencia de responsabilidades a las regiones?
- [ ] ¿Incluyen nuestras ofertas **compromisos a lo largo de todo el ciclo de vida** (por ejemplo, mantenimiento, actualizaciones, alineación con la hoja de ruta), y no sólo una entrega única?
- [ ] ¿Podemos lograr la **aceptación basada en el rendimiento** (por ejemplo, pruebas de funcionamiento, resultados medibles) sin excepciones específicas para cada proveedor?

La interoperabilidad y la capacidad de adaptación a gran escala superan a las características en una demostración, siempre.

Consideraciones estratégicas para profesionales (operadores y líderes en seguridad)

Integren la seguridad desde el principio. Integrar la seguridad después de haber tomado decisiones en materia civil, estructural, mecánica, eléctrica y de fontanería garantiza que se produzcan situaciones evitables. La participación temprana en materia de seguridad alinea el perímetro, el acceso y la vigilancia con los planos del sitio, los servicios públicos y los flujos de tráfico, lo que reduce los cambios en los pedidos y mejora los resultados.

Adopten una estrategia de integración múltiple regida por estándares. Dadas la velocidad y la geografía, rara vez basta con un solo socio. Las normas documentadas, las listas de productos aprobados y los procesos de certificación permiten que múltiples integradores trabajen de forma consistente. Mantengan una base de referencia actualizada y un proceso estricto para las excepciones y el control de versiones.

Alineen las fases de construcción con los riesgos de seguridad. La nueva norma, iluminar espacios parciales mientras las áreas adyacentes aún están en construcción, exige controles para entornos de construcción en funcionamiento: acceso por zonas, cobertura de vigilancia temporal, demarcaciones claras entre las zonas en "funcionamiento" y las de "construcción" y planes de actuación rápida ante incidentes.

Refuercen la rendición de cuentas en los procesos de adquisición. Pidan visibilidad de los subpedidos en relación con las especificaciones, incluidos los números de serie, las versiones de firmware y las listas de verificación de puesta en servicio. Vinculen la aceptación con el rendimiento demostrado, no sólo con la instalación. Siempre que sea posible, utilicen especificaciones basadas en el rendimiento con resultados medibles y pruebas de verificación.

Coordinen con las agencias policiales y los servicios de emergencia. Los protocolos de acceso planificados previamente, la interoperabilidad de radio y los ejercicios de simulación de escenarios evitan retrasos en situaciones de emergencia. Integren los requisitos de seguridad pública en el diseño del sitio (por ejemplo, acceso para vehículos de emergencia, rutas de evacuación, restricciones en el uso del agua).

Inviertan en las personas y en los procesos. La creciente brecha de habilidades afecta a todos los puestos, desde los equipos de seguridad de los usuarios finales hasta los integradores sobre el terreno. Implementen programas de formación interna, requisitos de certificación de proveedores y protocolos de escalamiento para la atención de incidencias. Aclaren las responsabilidades entre el personal de seguridad y el de construcción para la División 32 (obra) y el alcance de la seguridad para evitar el problema de que "todos son responsables y nadie lo es".

Mirando al futuro: Desafíos y oportunidades emergentes

La convergencia ciberfísica definirá la próxima década. La gestión de identidades en tiempo real, la correlación de eventos físicos y lógicos y la evaluación de riesgos serán la base para la toma de decisiones de acceso y la respuesta a incidentes en tiempo real. La frontera entre la "seguridad informática" y la "seguridad física" seguirá difuminándose.

La seguridad adaptativa definida por software está empezando a perfilarse. Las políticas, y no los dispositivos puntuales, serán las que orquesten las respuestas; la infraestructura se volverá más modular, con analíticas y automatización que absorberán las decisiones rutinarias y sólo remitirán las excepciones.

La gobernanza debe mantenerse al día. Las arquitecturas innovadoras se estancarán si no existen marcos normativos que reconozcan y guíen su uso. Los profesionales advierten que los modelos sólo tendrán éxito si se ajustan a las normas y a los controles de auditoría.

Por último, la cultura importa. El conocimiento obsoleto, los equipos aislados y la comunicación improvisada ralentizan el progreso. Las mesas redondas, las revisiones conjuntas de diseño y el aprendizaje compartido tras los incidentes entre usuarios finales, integradores y fabricantes elevan el nivel para todos, incluso entre la competencia. En un mercado en el que las consecuencias del fracaso se comparten, la colaboración no es altruismo, sino gestión de riesgos.

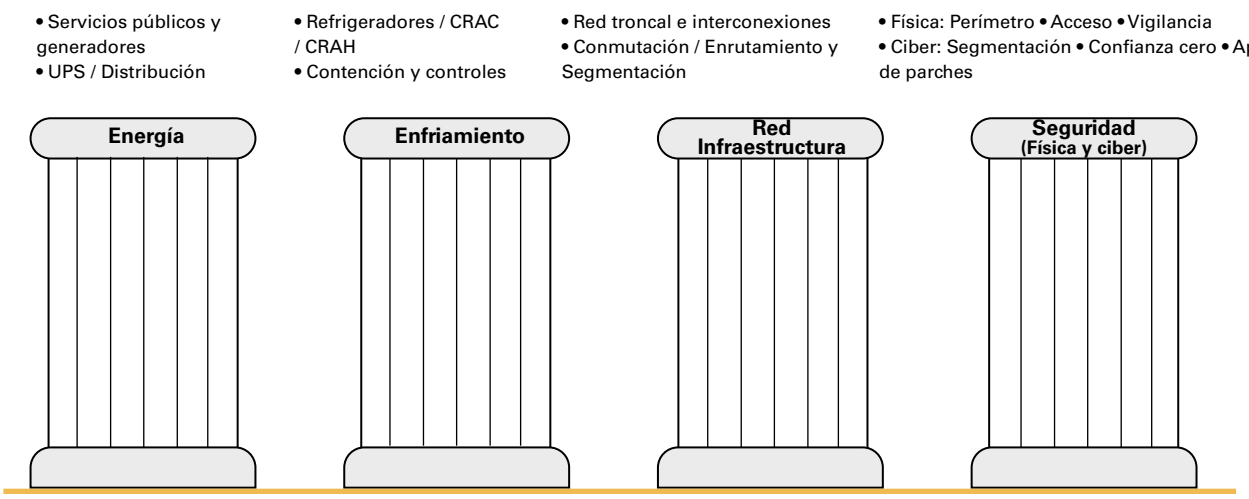
"Los modelos adaptativos sólo tendrán éxito si se ajustan a los marcos de cumplimiento y gobernanza, y si los equipos comparten las lecciones

Conclusión

La seguridad física ahora no se puede separar de la resiliencia, la confianza y la diferenciación competitiva en el mercado de los centros de datos. Los costos de tratarla como algo secundario superan con creces la inversión necesaria para integrarla desde el principio y gestionarla como un programa de ciclo de vida completo.

Los fabricantes e integradores deben ofrecer soluciones interoperables y basadas en API-first, demostrar su capacidad para escalar y estructurarse en torno a cuentas globales con ejecución regional. Los operadores deben integrar la seguridad en el diseño desde el primer día, regirse por estándares que permitan la participación de múltiples proveedores y alinear las fases de construcción con los riesgos de seguridad. Juntos, todos los interesados pueden transformar la seguridad física, para que pase de ser un simple requisito de cumplimiento a un factor clave para el éxito empresarial, y que respalde la velocidad, la escala y la fiabilidad que exigirá la próxima década de crecimiento digital.

Cuatro pilares: Energía • Refrigeración • Infraestructura de red • Seguridad



Estos cuatro pilares deben diseñarse conjuntamente para cumplir los objetivos de disponibilidad, rendimiento y gestión de riesgos.

PRODUCIDO CON EL APOYO DE

MOTOROLA SOLUTIONS

PAVION™
CONNECT AND PROTECT

PLUGOUT

SIA
SECURITY INDUSTRY ASSOCIATION

securityindustry.org

©2025 Security Industry Association.
Todos los derechos reservados.