

Guía para Infraestructura Crítica

Protege tu empresa respondiendo de manera rápida ante posibles brechas físicas de seguridad.

Los Retos que Enfrentas

Protege tu infraestructura crítica mediante múltiples capas de sistemas de seguridad física.

La infraestructura crítica enfrenta las mismas amenazas de seguridad que otros sectores, pero con consecuencias potencialmente mucho más graves para millones de personas. En esencia, la seguridad física consiste en proteger tus instalaciones, al personal y a los activos frente a amenazas del mundo real. Esto incluye la disuasión física, la detección de intrusos y la respuesta en tiempo real ante cualquier incidente.

Ataques Hostiles

Visitantes No Registrados

Acceso No Autorizado

Robo de Documentos

Robo de Servidores/Datos

Suplantación de Identidad

Vandalismo

Espionaje



Sectores Industriales Afectados

Centros de Datos



La seguridad física de un centro de datos comprende diversos tipos de características integradas de protección y seguridad diseñadas para resguardar las instalaciones y, con ello, el equipo que almacena datos críticos para aplicaciones multiusuario. Reducir los riesgos en un centro de datos implica medidas de prevención, control de acceso biométrico, detección de intrusos y videovigilancia, lo que permite una respuesta rápida ante eventos críticos.

Servicios Públicos



En Estados Unidos existen más de 55,000 subestaciones eléctricas, muchas de las cuales son objetivos atractivos debido a la función crítica que desempeñan y al hecho de que suelen estar desatendidas y ubicadas en zonas remotas. Tradicionalmente, la seguridad en subestaciones eléctricas se centraba únicamente en prevenir el acceso no autorizado, con el fin de evitar actos de vandalismo y mejorar la seguridad. Sin embargo, en la actualidad, los esfuerzos de seguridad se han redefinido para hacer frente a nuevas amenazas y proteger eficazmente esta infraestructura crítica.

Petróleo y Gas



Garantizar una seguridad física confiable y eficaz en el sector de petróleo y gas representa un desafío considerable, especialmente cuando las instalaciones se encuentran en ubicaciones remotas y, con frecuencia, de alto riesgo. Las tensiones geopolíticas han derivado en un aumento de los ataques terroristas dirigidos a la infraestructura física de esta industria, con el objetivo de ganar notoriedad y tomar control de los valiosos recursos que estas plantas procesan.

Operaciones de Minería y Canteras



Ya se trate de diamantes, oro, uranio o plomo, existe la necesidad de proteger los productos extraídos frente al robo o al terrorismo. Restringir el acceso a visitantes y personas no autorizadas requiere una planificación cuidadosa, así como la implementación de medidas de seguridad física y videovigilancia, lo cual puede ser un desafío cuando las operaciones se extienden sobre áreas vastas y de difícil control.

Instalaciones Gubernamentales



La seguridad física integral se ha vuelto fundamental para proteger las instalaciones, propiedades, información y personal de las agencias gubernamentales. La integración de videovigilancia, control de acceso y el poder de la analítica están transformando la seguridad física en instalaciones gubernamentales a nivel local, estatal y federal.



Adoptar un Enfoque por Capas

Un protocolo de seguridad exitoso va más allá de una entrada principal segura. La implementación de tecnologías inteligentes permite contar con instalaciones más completas y protegidas.

La mayoría de las empresas concentran toda la seguridad en la entrada principal: cámaras de vigilancia, guardias de seguridad y acceso con credencial; pero descuidan la protección del resto del edificio o instalación en su conjunto.



Seguridad Perimetral Desafíos

- Lograr el objetivo básico de identificar a las personas que entran y salen de la instalación.
- Monitoreo de zonas estériles para detectar personas que saltan cercas o se arrastran.
- Falsas alarmas que generan una carga operativa significativa para los guardias, quienes eventualmente terminan desactivando el sistema.

Con Oosto

- Tecnología propietaria basada en IA que combina reconocimiento facial, atributos corporales, objetos y personas.
- Ofrece una precisión inigualable incluso en entornos con poca luz, ángulos extremos o rostros parcialmente cubiertos.
- Proporciona una seguridad perimetral superior con la tasa más baja de falsas alarmas.
- Logra un aumento del 90% en la productividad del equipo de seguridad.



Control de Accesos Desafíos

- Conceder acceso a empleados y visitantes autorizados.
- Generar alertas si un visitante excede el tiempo permitido de estancia.
- Reducir el riesgo de exposición a COVID-19 asociado al contacto con superficies.

Con Oosto

- Reducir la carga de trabajo e incrementar la productividad en seguridad mediante alertas precisas, automatizadas y personalizables.
- Recibir notificaciones instantáneas ante accesos no autorizados.
- Proporcionar seguimiento en tiempo real de rutas y ubicación (para evitar que los visitantes accedan a zonas sensibles).
- Concluir investigaciones más rápidamente con búsquedas instantáneas por individuo y/o atributos personales.



Control Interno por Cuadrantes

Desafíos

- Controlar el acceso a espacios dentro de un edificio donde no existen puertas físicas o puntos de entrada definidos.
- Gestionar el acceso a zonas internas según el horario, el rol o los permisos asignados por grupo.
- Agregar una capa de autenticación doble o triple para áreas altamente sensibles dentro de la instalación.

Con Oosto

- Crear barreras efectivas sin necesidad de estructuras permanentes y recibir alertas instantáneas al identificar personas no autorizadas.
- Establecer fácilmente reglas sobre quién puede acceder a cada área mediante un motor de reglas granular, personalizable por horario, grupos y ubicación.
- La capacidad forense permite una investigación rápida y precisa ante cualquier incidente.



Control de Gabinetes y Racks

Desafíos

- Las cámaras se instalan sobre o dentro de los racks, pero requieren intervención humana para verificar que la persona correcta esté accediendo al rack.
- Se debe cumplir con lineamientos y prácticas que establecen quién está autorizado para abrir un gabinete en un momento determinado.

Con Oosto

- Recibir alertas automáticas cuando una persona no autorizada intente acceder a un gabinete o rack.
- Generar alertas por accesos fuera del horario permitido.
- Proporcionar información en tiempo real sobre la ubicación y el análisis de ruta de individuos no autorizados.



Para más información, por favor contáctanos en: info@thinksafe.com.mx

Oosto no ofrece, vende ni pone a disposición ninguno de sus productos o servicios a clientes en la Unión Europea para el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley, ni para ninguna de las demás prácticas de inteligencia artificial prohibidas según lo establecido en la Ley de IA de la UE.