Comisión Portuaria Nacional Guatemala

Autoridad Designada del Sistema Portuario Nacional

GUÍA TÉCNICA

DE FUNCIONALIDAD Y APLICACIÓN DE TECNOLOGÍAS PARA EL ROBUSTECIMIENTO Y MODERNIZACIÓN

DE PROTECCIÓN PORTUARIA

VERSIÓN 1

REPÚBLICA DE GUATEMALA, 2026

GUI-DPP-PIP-VMC-02

Autoridad Designada

del Sistema Portuario Nacional

Decreto 26-2024

Contenido

Puerto Santo Tomás de Castilla


COMISION PORTUARIA
CPN1003
1972
GUA502

Autoridad Designada del Sistema Portuario Nacional

Para la verificación del cumplimiento de las medidas de protección portuaria contenidas en el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias -PBIP-, Decreto Número 26-2024, Ley de la Autoridad Designada del Sistema Portuario Nacional.

PUERTOS DE GUATEMALA

Un puerto marítimo es una instalación costera destinada a facilitar el intercambio de mercancías y pasajeros entre embarcaciones y el transporte terrestre. Guatemala cuenta con tres puertos marítimos importantes distribuidos entre ambas costas: Santo Tomás de Castilla y Puerto Barrios en el litoral Caribe, y Puerto Quetzal en el litoral Pacífico. Estas instalaciones conforman los principales puntos de entrada y salida de comercio exterior del país y se interconectan mediante la red vial nacional.

En cuanto a su operación, los puertos comerciales del país están administrados por entidades públicas: Empresa Portuaria Quetzal, Empresa Portuaria Nacional Santo Tomás de Castilla y administración privada: Chiquita Guatemala, las cuales forman parte del Pleno de la Comisión Portuaria Nacional, según lo establece la Ley de la Autoridad Designada del Sistema Portuario Nacional. Estas organizaciones estatales y privadas gestionan la infraestructura, los servicios y la administración portuaria, constituyendo el eje público y privado del sistema marítimo nacional.

Océano
Atlántico

PUERTO BARRIOS
Operador

PUERTO SANTO TOMÁS DE CASTILLA
Operador

PUERTO QUETZAL
Operadores

Océano
Pacífico

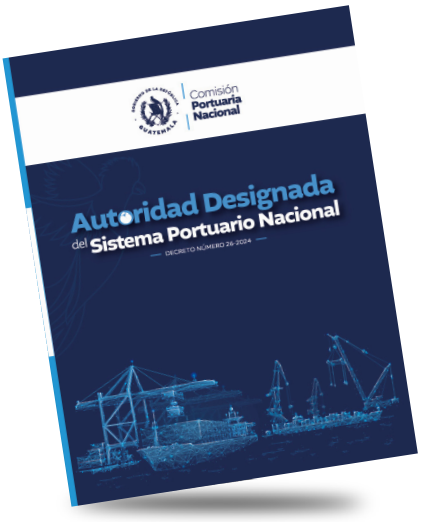
1 Introducción

La Autoridad Designada del Sistema Portuario Nacional -ADSPN-, por designación expresa del Estado de Guatemala, es el órgano técnico competente para velar por el cumplimiento de las regulaciones en materia de protección, asesoría y capacitación portuaria en el Sistema Portuario Nacional, para ello trabaja con la comunidad internacional de puertos de la Organización de Estados Americanos (OEA), Organización Marítima Internacional (OMI), Foro PBIP Internacional, Comité Interamericano Contra el Terrorismo (CICTE-OEA) y otras Autoridades Designadas de la región, en materia del Código Internacional para la Protección de Buques y de las Instalaciones Portuarias (Código PBIP), promoviendo el desarrollo de los puertos, la protección portuaria, asistencia técnica y fortalecimiento de las capacidades del personal portuario.

Como ente especializado, se promueve una “visión país” para articular esfuerzos y coordinaciones a efecto que los puertos nacionales, sean puertos competitivos, seguros y que contribuyan a la facilitación de comercio, respetando la autonomía y modelos de gobernanza de cada entidad y trabajando de manera colaborativa y organizada para brindar ese acompañamiento técnico necesario basado en las mejores prácticas internacionales.

02

Protección Portuaria



2.1 Objetivo

Brindar lineamientos e insumos técnicos a las entidades afectas al Código PBIP para orientar la identificación, evaluación, selección, implementación, integración, operación y mantenimiento de tecnologías avanzadas que fortalezcan sus sistemas de protección portuaria, con enfoque basado en riesgo, continuidad operativa, integridad de la información y mejora continua, en cumplimiento del Código PBIP, Parte A, secciones 15.5, 16.3 y 17.2.12, Parte B, secciones 16.49 a 16.53; del Decreto 26-2024, Ley de la Autoridad Designada del Sistema Portuario Nacional, especialmente sus artículos 6, 8, 9, 10, 13, 20 y 21; y del Acuerdo Gubernativo 112-2021, artículo 16, relativo a normas, directrices y parámetros armonizados para la implementación de medidas y tecnologías de protección portuaria.

2.2 Alcance

El alcance de esta Guía está orientado a brindar información para robustecer con tecnologías los procesos que contemplan los Planes de Protección de las Instalaciones Portuarias (PPIP) siguientes:

1. Acceso a la instalación portuaria.
2. Zonas restringidas.
3. Manipulación de la carga.
4. Vigilancia de protección de la instalación portuaria.

03

Orientación Técnica de Tecnologías para Robustecer la Protección en las Instalaciones Portuarias

3 Orientación
Técnica de Tecnologías

Para abordar los siguientes sucesos, amenazas y fallos en la protección que enfrentan actualmente las instalaciones portuarias de Guatemala, es necesario con adoptar medidas de reacción contra la diversidad de riesgos actuales, por ello es primordial prevenir y contar con una preparación para enfrentar cualquier amenaza futura. La tecnología desempeña un papel clave en este sentido, ya que permite al sector portuario una opción para reducir los riesgos emanados de las amenazas, fallas humanas, comunicación e inclusive la reducción de tiempos y costos. Esta Guía presenta producto de la identificación de mejores prácticas y las aplicaciones de las diversas tecnologías a nivel global en instalaciones portuarias aplicadas en las instalaciones portuarias.

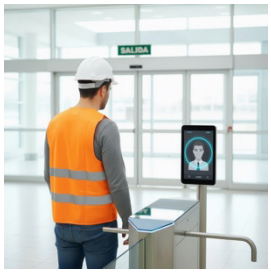
3.1.1 Control de Accesos

El control de accesos, contenido en la Parte A (14.2–14.4 y 16) y Parte B (16.17-16.20) del Código PBIP, el control de accesos es una medida obligatoria del Plan de Protección de la Instalación Portuaria tiene como propósito garantizar que únicamente personas, vehículos y cargas debidamente autorizadas ingresen o egresen de la instalación portuaria. Es la primera barrera activa del sistema de protección.

A. Biometría (facial, huella dactilar, iris)

Permite verificar la identidad del personal, conductores y visitantes de forma automatizada, eliminando el riesgo de suplantación mediante documentos o credenciales físicas. Se aplica en torniquetes peatonales, garitas vehiculares y accesos a zonas restringidas. Los sistemas modernos pueden operar en condiciones de baja iluminación y se integran fácilmente con bases de datos de personal y listas de restricción. Se recomienda su uso combinado con una credencial adicional (tarjeta o PIN) en zonas de mayor sensibilidad.

Las tecnologías de protección portuaria pueden organizarse según su función dentro del sistema de seguridad. A continuación, se describen las principales categorías, con sus tecnologías asociadas, ventajas y consideraciones de implementación.

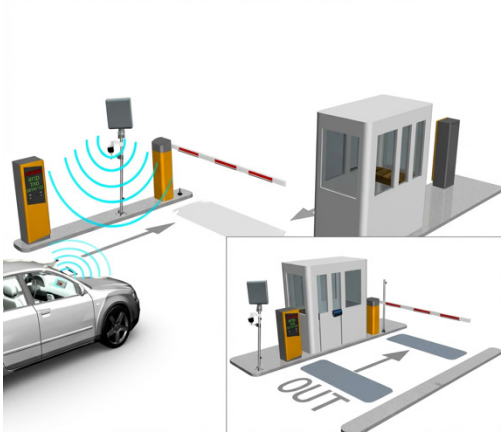


B. LPR (lectura automática de placas) y OCR (lectura de contenedores)

El LPR permite identificar automáticamente los vehículos que ingresan o egresan, validándolos en tiempo real contra listas de vehículos autorizados o de interés. El OCR aplicado a contenedores lee el código de identificación único de cada unidad de carga, agilizando el proceso de validación en portones sin intervención manual. Ambas tecnologías generan registros permanentes de todos los movimientos, con hora exacta y evidencia fotográfica.

C. RFID

La tecnología RFID permite identificar personas, vehículos o equipos mediante etiquetas electrónicas que se leen sin contacto, agilizando el control de accesos y el registro de movimientos dentro de la instalación portuaria. Su uso mejora la eficiencia operativa, reduce errores y fortalece la supervisión requerida por los estándares de protección portuaria, al permitir un control rápido y confiable de quién y qué ingresa o sale de la instalación portuaria.



D. Marchamos inteligentes

Los marchamos inteligentes son sellos electrónicos que permiten supervisar la integridad de los contenedores durante todo su tránsito. Su función es detectar y reportar cualquier intento de apertura no autorizada, reforzando la seguridad de la carga dentro del entorno portuario.

- Tecnologías que incorporan:
- RFID: para identificación y lectura rápida del sello.
- GPS/GNSS: para ubicación continua y trazabilidad de la ruta.
- Sensores de apertura o ruptura: alertan intentos de manipulación.
- Alertas en tiempo real: envían notificaciones inmediatas al sistema de control.

E. Cámaras térmicas en accesos

Detectan presencia de personas ocultas en el interior de vehículos mediante la diferencia de temperatura corporal respecto al entorno, sin necesidad de apertura física. Son especialmente útiles para la detección de polizones y el control de cargas con cavidades ocultas.

Ventajas generales

- Automatización del proceso de verificación, reduciendo tiempos de espera.
- Eliminación de errores propios del control manual.
- Generación de registros auditables de todos los movimientos.
- Reducción del riesgo de corrupción o complicidad en puntos de acceso.

Consideraciones de implementación

- Requieren integración con una base de datos centralizada y actualizada de personal y vehículos autorizados.
- La calidad y mantenimiento de los datos es determinante para la efectividad del sistema.
- Se recomienda establecer procedimientos claros de enrolamiento, actualización y revocación de accesos.

3.1.2 Monitoreo Perimetral

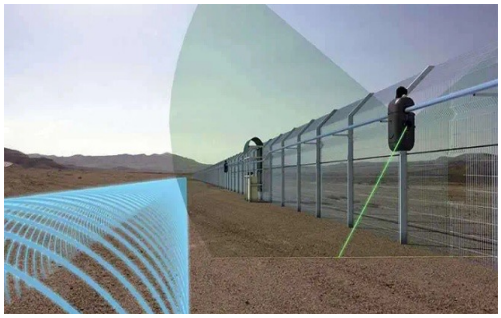
El monitoreo perimetral, contenido en la Parte A (14.2) y parte B (16.49-16.54) del Código PBIP, busca detectar de forma temprana cualquier intento de acceso no autorizado a través de los límites físicos de la instalación, tanto por vía terrestre como acuática.

A. PIDS (Sistemas de Detección de Intrusión Perimetral)

Incluyen sensores instalados sobre la valla o estructura perimetral de fibra óptica, microfónicos o sísmicos que detectan intentos de corte, escalamiento o manipulación. Permiten localizar con precisión el punto donde se produce el evento, orientando la respuesta hacia el sector afectado. Su principal ventaja es que operan de forma invisible para el intruso y son difíciles de evadir sin generar una alerta.

B. Barreras infrarrojas y de microondas

Generan un campo de detección entre un emisor y un receptor. Cualquier interrupción de dicho campo activa una alerta. Son adecuadas para proteger accesos secundarios, pasillos y zonas de transición entre áreas de distinto nivel de restricción.



C. Radar terrestre

Permite detectar movimiento en áreas extensas —incluyendo el frente acuático— con independencia de las condiciones de luz o clima. Identifica personas, vehículos o embarcaciones antes de que alcancen el límite físico de la instalación, proporcionando mayor margen de tiempo para la respuesta. Se integra directamente con cámaras PTZ, a las que dirige automáticamente hacia el punto donde se detecta el movimiento.

D. Cámaras térmicas y PTZ perimetrales

Las cámaras térmicas detectan presencia sin necesidad de iluminación, no se ven afectadas por sombras ni reflejos y operan en condiciones de niebla o lluvia. Las cámaras PTZ complementan su función con imagen a color de alta resolución para la identificación positiva del intruso. La combinación de ambas tecnologías permite tanto la detección como la verificación del evento.

Ventajas generales

- Detección temprana antes de que la amenaza ingrese a la zona operacional.
- Cobertura continua sin depender de la atención del personal.
- Capacidad de cubrir frentes extensos, incluyendo zonas acuáticas.

Consideraciones de implementación

- Los sensores perimetrales requieren calibración adecuada al entorno para minimizar falsas alarmas.
- Las condiciones climáticas locales deben considerarse en el diseño del sistema.
- Se recomienda prever mantenimiento preventivo periódico

3.1.3 Vigilancia Inteligente

La vigilancia inteligente, contenido en la Parte A (14.2) y Parte B (16.49-16.54) del Código PBIP, comprende los sistemas que optimizan la supervisión mediante automatización, analítica y el uso de inteligencia artificial, reduciendo la dependencia de la atención humana continua.

A. Analítica de video con inteligencia artificial

Los sistemas de analítica procesan automáticamente las imágenes de las cámaras en tiempo real, generando alertas ante eventos predefinidos sin necesidad de que un operador observe continuamente las pantallas. Entre las funciones más útiles para entornos portuarios se encuentran: detección de merodeo en zonas restringidas, cruce de líneas virtuales, detección de vehículos detenidos en lugares no autorizados, objetos abandonados y reconocimiento de personas o placas de interés. Su principal valor es permitir que un número reducido de operadores supervise eficazmente una instalación con múltiples cámaras activas.

B. Drones (UAS — Sistemas Aéreos No Tripulados)

Acorde a lo que establece el Código PBIP en la Parte B (16.49.3) “Desde la propia instalación se debe poder vigilar en todo momento, incluso en la oscuridad y con visibilidad limitada, toda la instalación portuaria, los accesos por mar y tierra, las zonas restringidas...,” se permite el patrullaje dinámico de zonas extensas, incluyendo el frente marítimo y áreas de difícil acceso para el personal terrestre. Pueden operar en rutas programadas o ser despachados de forma reactiva ante una alerta específica, llegando al punto del evento en segundos y transmitiendo imágenes en tiempo real al centro de monitoreo. Complementan la vigilancia estática de cámaras fijas con una perspectiva aérea que ningún sensor en tierra puede proporcionar.

C. Centros de monitoreo integrados

Constituyen el punto de convergencia de toda la información generada por los sistemas de seguridad. Desde un centro de monitoreo correctamente equipado, un equipo reducido de operadores puede supervisar en tiempo real el estado de la instalación, gestionar alertas, coordinar la respuesta ante incidentes y mantener comunicación con unidades internas y organismos externos. Su efectividad depende directamente de la integración de los sistemas que alimentan la información y de la capacitación del personal que los opera.

Ventajas generales

- Reducción significativa de la dependencia del factor humano en la detección.
- Generación de alertas en tiempo real con mínima intervención del operador.
- Capacidad de cobertura de grandes áreas con recursos humanos limitados.

Consideraciones de implementación

- Requieren infraestructura de red y comunicaciones estable.
- El personal de operación debe recibir capacitación específica en el uso de las plataformas.
- Los parámetros de analítica deben ajustarse al contexto operacional específico de cada instalación.

3.1.4 Control de Carga

El control de carga, contenido en el Código PBIP, Parte A (14.2) y Parte B (16.30-16.37), busca garantizar la integridad de la cadena logística, previniendo el ingreso o egreso de mercancías ilícitas, el contrabando y la manipulación de cargas y otros delitos transfronterizos, esto como parte de las iniciativas y proyectos de las Autoridades Competentes, tales como Ministerio de Gobernación, Ministerio de Agricultura, Ganadería y Alimentación, Superintendencia de Administración Tributaria y otras que ejercen controles sobre las mercancías.

A. Escáneres no intrusivos (NII)

Permiten inspeccionar el contenido de contenedores y vehículos mediante rayos X de alta energía, sin necesidad de apertura física. Las imágenes resultantes muestran la distribución interna de la carga, permitiendo identificar anomalías como compartimentos ocultos, objetos extraños o personas. Su uso, orientado por criterios de perfilado de riesgo, permite aumentar significativamente el volumen de carga inspeccionada sin crear cuellos de botella operacionales. Los modelos más avanzados incorporan análisis asistido por inteligencia artificial para apoyar al operador en la interpretación de imágenes.

B. Sistemas de detección portátil (densímetros tipo Buster)

Dispositivos de mano que detectan variaciones de densidad en paneles, puertas, suelos y techos de vehículos, identificando posibles cavidades con materiales ocultos. Su portabilidad los hace complementarios ideales de los escáneres fijos, permitiendo inspecciones rápidas y dirigidas en campo.

C. Marchamos inteligentes (RFID/GPS)

Garantizan la integridad física del contenedor durante todo su tránsito, registrando cualquier apertura no autorizada y transmitiendo la posición en tiempo real. Permiten detectar desvíos de ruta y garantizar que el contenedor que ingresa al puerto es el mismo que fue cargado en origen, sin manipulaciones intermedias.

3.1.5 Tecnologías
Emergentes y Complementarias

Estas tecnologías no son exclusivas de la seguridad, pero ofrecen capacidades habilitadoras de alto valor cuando se integran al ecosistema de protección portuaria.

A. IoT — Internet de las Cosas

Red de sensores interconectados que generan datos continuos sobre condiciones ambientales, estado de equipos, presencia en zonas específicas y condición de cargas. Permite el monitoreo en tiempo real de variables que de otro modo requieren inspección manual periódica, como temperatura en almacenes, presencia de gases o estado de infraestructura crítica.

B. Plataformas PSIM (Gestión Integrada de Seguridad Física)

Software que integra en una sola interfaz todos los sistemas de seguridad —videovigilancia, control de accesos, sensores perimetrales, alarmas, comunicaciones— permitiendo al operador gestionar la totalidad de la instalación desde un punto único. Su principal valor no es solo agregar información, sino correlacionar eventos de distintos sistemas para generar alertas de mayor precisión que ningún sistema individual podría producir por sí solo.

C. Inteligencia artificial predictiva

Analiza datos históricos y en tiempo real para identificar patrones de riesgo antes de que se materialicen en incidentes. Aplicaciones relevantes incluyen el perfilado automatizado de riesgo de cargas y la detección de comportamientos anómalos recurrentes en personas o vehículos.

D. AIS — Sistema de Identificación Automática de Buques

Sistema de rastreo que transmite y recibe información de posición, identidad, rumbo y velocidad de embarcaciones. Su integración con los sistemas de seguridad del puerto permite identificar anticipadamente los buques que se aproximan, detectar embarcaciones que operan sin identificación activa y cruzar la información con listas de alerta o sanciones internacionales.

3.2 Uso Estratégico: Modelo de Anillos de Protección

Las tecnologías descritas adquieren su máximo valor para robustecer la protección portuaria cuando se organizan estratégicamente bajo un modelo de defensa en profundidad, donde los controles se distribuyen en capas progresivas. Este modelo, conocido como sistema de tres anillos dentro de la instalación portuaria, garantiza que incluso si una capa es superada, las siguientes mantienen la capacidad de detectar y responder a la amenaza.

A. Anillo 1 — Perímetro de la instalación portuaria

Objetivo:

Detectar y disuadir amenazas antes de que ingresen a la instalación.

Este anillo cubre la línea física del perímetro terrestre y el frente acuático. Las tecnologías desplegadas aquí buscan generar la alerta más temprana posible, con suficiente anticipación para que la respuesta pueda ser efectiva.

Las tecnologías clave son los PIDS, el radar, las cámaras térmicas de largo alcance y los drones. Ante una detección, el sistema debe ser capaz de verificar automáticamente el evento mediante cámara o dron dirigido al punto exacto y activar el protocolo de respuesta correspondiente, sin necesidad de que el operador esté observando activamente en ese momento.

B. Anillo 2 — Área Operacional

Objetivo:

Controlar y rastrear el flujo de personas, vehículos y carga dentro de la instalación.

Este anillo actúa sobre quienes ya han ingresado a la instalación, garantizando que cada persona, vehículo y unidad de carga esté identificada, autorizada y monitoreada durante toda su permanencia.

Las tecnologías clave son la biometría en puntos de control internos, el LPR/OCR para seguimiento vehicular, el RFID para trazabilidad de contenedores, la analítica de comportamiento y los escáneres NII en portones de salida. La efectividad de este anillo depende en gran medida de la integración entre el sistema de seguridad y el sistema logístico del puerto, de modo que cualquier discrepancia entre lo declarado y lo verificado genere una alerta automática.

C. Anillo 3 — Activos Críticos

Objetivo:

Proteger la infraestructura y los sistemas de mayor valor estratégico de la instalación.

Este anillo aplica los controles más estrictos sobre los activos cuya afectación comprometería directamente la operatividad del puerto o la seguridad nacional: sala de control, servidores y sistemas informáticos, subestaciones eléctricas, depósitos de mercancías peligrosas o de alto valor.

Las tecnologías clave incluyen biometría con autenticación multifactor, mantraps (esclusas de doble puerta que impiden el acceso simultáneo de personas no autorizadas), videovigilancia sin ángulos ciegos y sistemas de ciberseguridad para la protección de redes y sistemas de control industrial. El acceso a estas zonas debe estar limitado al mínimo de personal estrictamente necesario, con registros completos de cada ingreso.

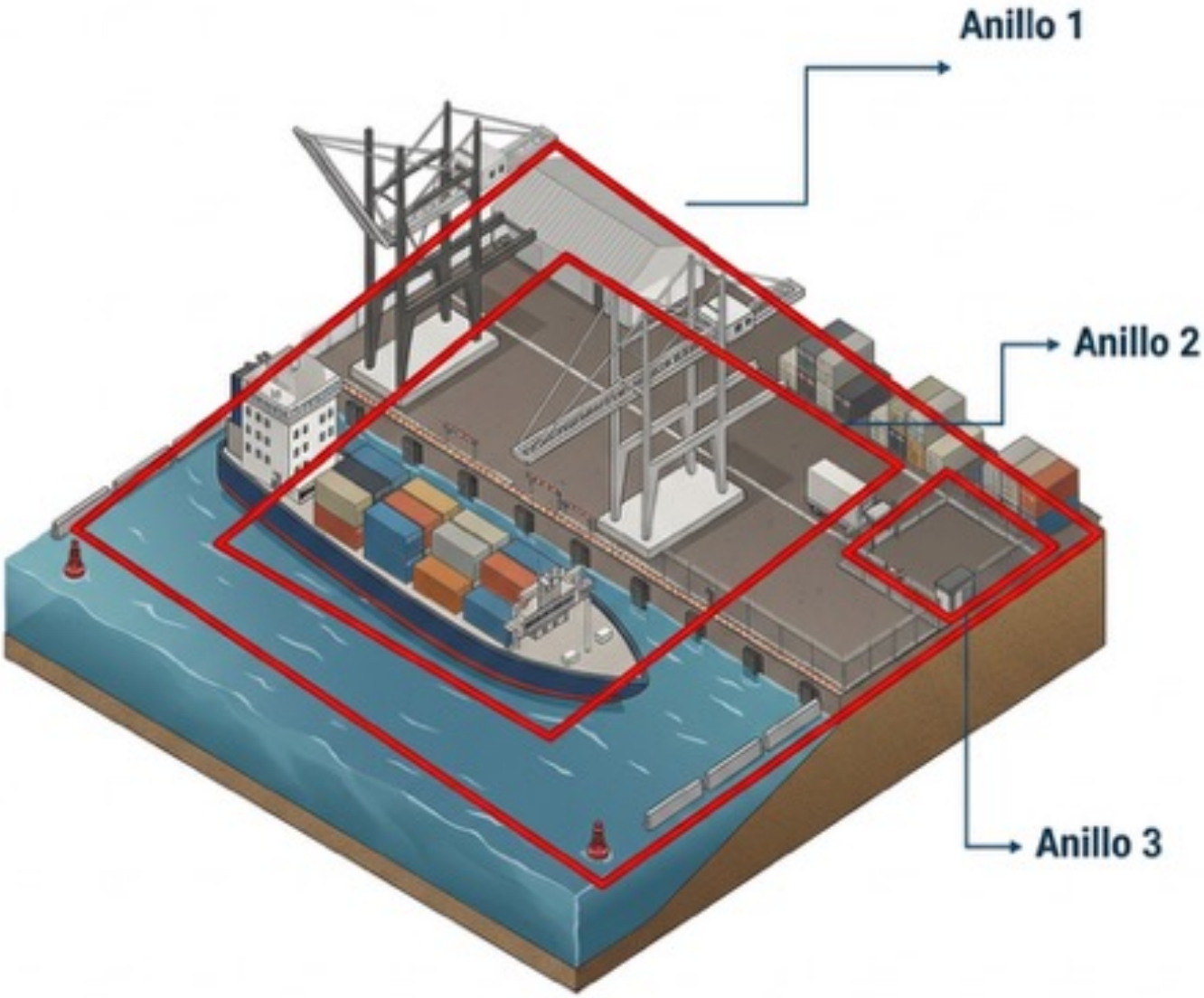
D. Integración entre anillos

El valor del modelo reside en que los tres anillos operan de forma coordinada. Una alerta generada en el Anillo 1 puede activar controles adicionales en el Anillo 2; una anomalía detectada en el Anillo 2 puede desencadenar el cierre preventivo de accesos en el Anillo 3. Esta coordinación, gestionada desde el centro de monitoreo mediante una plataforma PSIM, convierte al sistema en algo significativamente más robusto que la simple suma de sus partes.

E. Anillo orbitante: Coordinación con Autoridades competentes

Como complemento a los anillos internos, la protección portuaria requiere coordinación permanente con las autoridades e instituciones que ejercen competencias en seguridad, control, fiscalización, migración, aduanas, defensa e investigación. Este nivel fortalece la capacidad preventiva y de respuesta de la instalación mediante el intercambio oportuno de información, la articulación institucional y la atención coordinada de incidentes y riesgos relevantes.

Modelo
de Anillos de Protección



3.3 Matriz de Tecnologías por Función y Anillo de Protección

Las siguientes matrices organizan las tecnologías aplicables a la protección portuaria conforme a dos criterios: la función que cumplen dentro del sistema de protección, es decir, disuadir, detectar, demorar y responder; y el nivel de protección en el que resultan más útiles dentro de la instalación portuaria, comprendiendo el perímetro, el área operacional y los activos críticos.

Este esquema facilita visualizar de qué manera cada tecnología aporta a una protección integral de la instalación portuaria, permitiendo identificar fortalezas, vacíos y oportunidades de mejora en cada nivel. Su utilidad práctica radica en apoyar la planificación, priorización e integración de medidas tecnológicas dentro de los Planes de Protección de las Instalaciones Portuarias, considerando el enfoque basado en riesgo y el principio de protección en profundidad previsto en el Código PBIP.

La matriz también permite relacionar las necesidades operativas de cada instalación con las soluciones tecnológicas disponibles, favoreciendo decisiones más consistentes en materia de inversión, implementación y mejora continua. En ese sentido, constituye un insumo técnico para orientar procesos de evaluación, auditoría, supervisión y actualización de medidas de protección portuaria.

A. Anillo 1 – Perímetro de la instalación portuaria

El primer anillo de protección comprende el perímetro terrestre y acuático de la instalación portuaria, así como sus accesos y zonas de aproximación. Su objetivo es disuadir, detectar y contener de forma temprana cualquier intento de ingreso no autorizado, generando el tiempo necesario para verificar el evento y activar la respuesta correspondiente.

ANILLO 1 -PERIMETRO DE LA INSTALACIÓN PORTUARIA			
DISUADIR	**DETECTAR**	**DEMORAR**	**RESPONDER**
Iluminación inteligente activada por movimiento	PIDS — Fibra óptica en cerca	Bolardos hidráulicos certificados K12	PTZ con auto-tracking de objetivos
PA / Voz automatizada de advertencia	Barreras microondas / IR activas	Speed Gates / Torniquetes rápidos	Unidades móviles de respuesta rápida
Patrullas K-9	Cámaras térmicas perimetrales	Coronaciones anti-escalada en cerca	Drones (UAS) de respuesta ante alerta
Señalización de alta seguridad	LPR / ANPR (lectura de placas)	Chicanes / Barreras vehiculares en acceso	Comunicaciones de emergencia integradas
Cercas de alta seguridad visibles	Radar terrestre y marítimo	Fosas de seguridad (tiger traps)	Coordinación con Policía / Guardia Costera
Vehículos de patrullaje visibles	Sensores sísmicos subterráneos	Cables de acero en perímetro acuático	Centro de comando móvil de emergencia
	Drones de reconocimiento perimetral		
	Detectores de drones no autorizados (C-UAS)		

B. Anillo 2 – Operacional

El segundo anillo corresponde al área donde se desarrollan las operaciones diarias de la instalación portuaria, incluyendo el movimiento de personas, vehículos, carga y equipos. Su finalidad es asegurar que todo tránsito interno se realice de forma autorizada, controlada y trazable, reduciendo riesgos de acceso indebido, manipulación no autorizada o desviaciones en la operación.

ANILLO 2 - OPERACIONAL			
DISUADIR	**DETECTAR**	**DEMORAR**	**RESPONDER**
Pases / Badges visibles con foto	Analítica de video (merodeo, cruce de línea)	Bloqueos remotos de acceso vehicular	Sistemas de mustering / conteo de personal
Monitores de vista pública (CCTV visible)	Escáneres NII / Rayos X en portones	Compartimentación de zonas operacionales	Notificación masiva (radio, SMS, altavoces)
Políticas conductuales y señalización interna	Tracking RTLS (posicionamiento en tiempo real)	Torniquetes de altura (full-height)	Procedimientos de bloqueo (lockdown)
Semáforos de zona (rojo/verde/amarillo)	Acceso biométrico en zonas operacionales	Doble validación de identidad en puntos clave	Evacuación guiada por iluminación de emergencia
Uniformes y chalecos identificadores	OCR de contenedores en portones	Esclusas de vehículos (vehicle airlocks)	Cierre automático de portones ante alerta
Avisos de videovigilancia activa	Marchamos electrónicos RFID/GPS	Control de velocidad interno (reductores)	PSIM — Gestión integrada de incidentes
	Densímetros portátiles (tipo Buster)		
	Sensores de apertura en contenedores		

C. Anillo 3 – Activos Críticos

El tercer anillo está orientado a proteger las áreas, infraestructuras y sistemas cuya afectación podría comprometer la continuidad operativa, la integridad de la carga, la protección de las personas o la capacidad de respuesta de la instalación. En este nivel deben aplicarse los controles más estrictos, limitando el acceso al personal estrictamente autorizado y manteniendo supervisión y registro permanente.

Nota: Esta matriz sigue el modelo Función × Anillo, donde cada celda responde a la pregunta: ¿Qué tecnología cumple esta función (Disuadir / Detectar / Demorar / Responder) en este nivel de la instalación (Perímetro / Operacional / Activos Críticos)? Su uso conjunto garantiza una cobertura integral bajo el principio de defensa en profundidad.

Anillo 3 — Activos Críticos			
DISUADIR	**DETECTAR**	**DEMORAR**	**RESPONDER**
Mantraps / Portales de seguridad	IDS — Detección de intrusiones en redes OT/SCADA	Puertas reforzadas con clasificación balística	Auto-failover y respaldo de sistemas críticos
Señalización “Zona Roja” / Acceso Restringido	Sensores ambientales (gas, temperatura, humedad)	Air-Gaps selectivos en redes críticas	Respuesta ciber-física coordinada
Política Zero Trust (sin confianza implícita)	SIEM Físico-Lógico (correlación de eventos)	MFA — Autenticación de múltiple factor	Supresión automática de incendios en sala técnica
Privacidad de datos y gestión de credenciales	Biometría de alto nivel (iris / vena de palma)	Cajas fuertes / Cofres para equipos críticos	Activación de protocolos de continuidad operativa
Auditoría de accesos en tiempo real	Detectores de radiación / CBRN	Segmentación de redes (VLAN / microsegmentación)	Aislamiento remoto de sistemas comprometidos
Rotación periódica de credenciales y PINs	Análisis de comportamiento de usuarios (UEBA)	Bloqueo automático ante alerta de intrusión	Notificación automática a autoridades externas
	Monitoreo de tráfico de red OT (anomalías)		
	Cámaras 360° sin ángulos ciegos en sala de control		


OOCL
Seacastle
TRITON
Toulax

04

Registro, Integración y Uso de la Información Generada

4 Información Generada

La información generada por los sistemas tecnológicos representa un activo estratégico de la instalación. Su adecuado registro, integración y uso es determinante tanto para la gestión operativa como para el cumplimiento normativo y la mejora continua.

A. Generación de datos

Los sistemas tecnológicos generan continuamente información sobre identidad de personas, movimientos de vehículos y carga, eventos de seguridad y operaciones logísticas. El volumen de esta información puede ser considerable en instalaciones de mediana y gran escala, lo que exige que su gestión esté prevista desde el diseño del sistema.

B. Registro de información

Toda la información relevante debe ser registrada de forma estructurada, con indicación de fecha y hora exacta, sistema de origen y, cuando corresponda, el operador que atendió el evento. Los registros deben almacenarse en sistemas que garanticen su integridad —es decir, que no puedan ser alterados una vez creados— y su disponibilidad ante cualquier requerimiento de auditoría o investigación.
Se recomienda definir plazos mínimos de retención según el tipo de información: los registros de control de acceso y los eventos de seguridad deben conservarse por períodos que permitan su uso en investigaciones posteriores, considerando los plazos procesales aplicables en la legislación guatemalteca.

C. Integración de sistemas

La mayor debilidad de muchos sistemas de seguridad portuaria no es la ausencia de tecnología, sino la falta de integración entre sistemas que operan de forma aislada. Se recomienda que las instalaciones avancen progresivamente hacia una arquitectura integrada donde la videovigilancia, el control de accesos, los sensores perimetrales y los sistemas logísticos compartan información en tiempo real a través de una plataforma centralizada.

Esta integración no requiere reemplazar todos los sistemas existentes simultáneamente; puede lograrse de forma gradual mediante el uso de plataformas de middleware o PSIM que actúan como capa de integración sobre sistemas ya instalados.

D. Uso de la información

La información registrada debe utilizarse activamente para tres propósitos principales:

- Toma de decisiones en tiempo real: proporcionar al operador del centro de monitoreo información procesada y contextualizada que reduzca el tiempo de respuesta ante incidentes.
- Análisis de patrones: identificar tendencias, zonas o períodos de mayor riesgo, y evaluar la efectividad real de los controles desplegados.
- Investigación post-incidente: permitir la reconstrucción forense de eventos para apoyar investigaciones internas y, cuando corresponda, judiciales.

E. Trazabilidad y cumplimiento del Código PBIP

Un sistema de registro adecuado facilita significativamente la demostración del cumplimiento de los requisitos del Código PBIP durante auditorías y verificaciones. Los registros digitales generados por los sistemas tecnológicos constituyen evidencia objetiva de qvue los controles están activos y operativos, complementando la documentación formal del Plan de Protección de la Instalación Portuaria.

F. Interoperabilidad institucional

La protección portuaria efectiva trasciende los límites de la instalación. El intercambio oportuno de información entre la instalación portuaria y las instituciones con competencia en seguridad —Aduana, Guardia Costera, Policía Nacional Civil, organismos de inteligencia— multiplica la efectividad de los controles individuales. Se recomienda que las instalaciones establezcan canales formales de comunicación y protocolos de intercambio de información con estas instituciones, incluyendo la definición de qué datos se comparten, en qué condiciones y bajo qué resguardos de confidencialidad.

5 Consideraciones Finales

A. El Código PBIP establece medidas generales, sin entrar a desarrollar a nivel de detalle tipologías de tecnologías, pero que producto de la interacción de mejores prácticas se ha cumplido esta. La protección portuaria es un proceso dinámico que requiere constantes cambios derivado de las innovaciones tecnológicas y de la evolución de los sucesos, amenazas y fallos.

B. Aplicabilidad de la inteligencia artificial y otras tecnologías, las cuales han revolucionado numerosos campos y la protección no es una excepción, cuya aplicación específicamente en el contexto del Código PBIP, plantea tanto oportunidades como desafíos.

C. Las amenazas que afectan a las instalaciones portuarias, son de carácter transnacional, afectando no solo al propio país, sino a la región, por lo que el uso de tecnología permite facilitar el intercambio de información oportunamente, con otras autoridades y organismos nacionales e internacionales.

D. Este compendio técnico no regulatorio y las funcionalidades presentes de los diferentes en la protección portuaria, como una guía para los Oficiales de Protección de las instalaciones Portuarias en las preparaciones de sus Planes de Protección de las Instalaciones Portuarias y medidas, y estimarlo conveniente que la Alta Dirección gestione la inclusión de estas tecnologías en los Planes Operativos Anuales (POA) y presupuestos 2026.

6 Definiciones
Técnicas

1. **Biometría:** Tecnología que identifica personas mediante rasgos físicos únicos.
2. **LPR:** Sistema de lectura automática de placas vehiculares.
3. **OCR:** Lectura automática de códigos de contenedores.
4. **RFID:** Identificación por radiofrecuencia para trazabilidad.
5. **Marchamos electrónicos inteligentes:** Sellos con RFID/GPS.
6. **Cámaras térmicas:** Detectan diferencias de temperatura.
7. **PIDS:** Sistemas de detección de intrusión perimetral.
8. **Barreras infrarrojas:** Sensores que generan un campo de detección.
9. **Barreras de microondas:** Campo volumétrico para detección.
10. **Radar terrestre/marítimo:** Detección de movimiento a distancia.
11. **Cámaras PTZ:** Cámaras motorizadas con zoom.
12. **Analítica de video con IA:** Detección automática de eventos.
13. **Drones UAS/RPAS:** Patrullaje y vigilancia aérea.
14. **Centros de monitoreo integrados:** Sala de control centralizada.
15. **Escáneres NII:** Rayos X para inspección sin apertura.
16. **Densímetros portátiles:** Detectan cavidades ocultas.
17. **IoT:** Red de sensores conectados.
18. **PSIM:** Plataforma de gestión integrada de seguridad.
19. **IA predictiva:** Identificación anticipada de riesgos.
20. **AIS:** Sistema de identificación automática de buques.
21. **Mantraps:** Esclusas de doble puerta.
22. **Air-Gap:** Separación física entre redes.
23. **MFA:** Autenticación multifactor.
24. **VLAN/Microsegmentación:** División de redes.
25. **SIEM físico-lógico:** Correlación de eventos de seguridad.

GOBIERNO DE LA REPÚBLICA · GUATEMALA

Comisión
Portuaria Nacional

Autoridad Designada
del **Sistema Portuario Nacional**