Autoridad Designada
del Sistema Portuario Nacional

GUÍA TÉCNICA

DE FUNCIONALIDADES Y APLICACIÓN DE TECNOLOGÍAS PARA EL ROBUSTECIMIENTO DE LA

PROTECCIÓN PORTUARIA

VERSIÓN III

República de Guatemala, 2026
GUI-DPP-PIP-VMC-02

Autoridad Designada
del Sistema Portuario Nacional

Contenido

01
Introducción **11**

02
Protección Portuaria **13**
2.1 Objetivo 13
2.2 Alcance 13

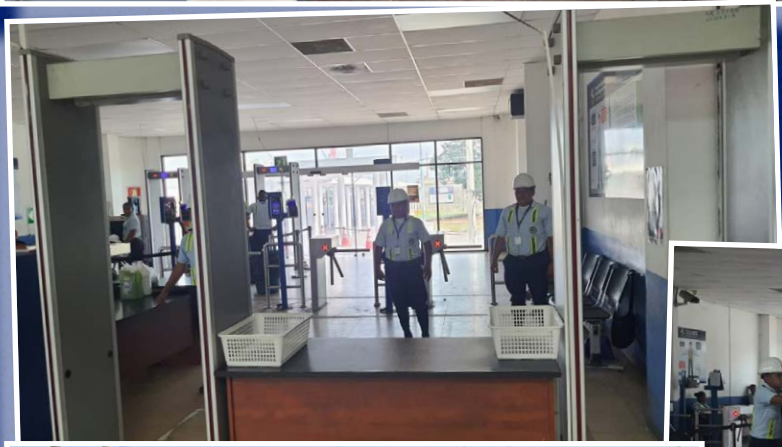
03
Tecnologías para la Protección Portuaria **15**
3.1 Tecnologías Aplicables a la Protección Portuaria 17
3.1.1 Sistemas no tripulados 17
3.1.2 Cámaras de videovigilancia 18
3.1.3 Sistemas de control de acceso 20
3.1.4 Sistemas de detección de intrusión 21
3.1.5 Sistemas de inspección no intrusiva 22
3.1.6 Sistemas de sellado y trazabilidad 23
3.1.7 Sistemas de disuasión 24
3.1.8 Software 25

04
Modelo de Anillos para Proteger la Instalación Portuaria **27**
4.1 Orientación Técnica de Tecnologías 27
4.2 Modelo de Anillos de Protección 27
4.3 Matriz de Tecnologías Avanzadas 31
4.3.1 Anillo 1 - Perímetro de la instalación portuaria 32
4.3.2 Anillo 2 - Áreas operacionales 33
4.3.3 Anillo 1 - Áreas o activos críticos 34

05
Información Generada **37**

ANEXOS
Definiciones Técnicas 39
Uso de Tecnologías Dispersas vrs. Ecosistemas de Protección 40

Modelo de Control de acceso peatonal EPQ



Autoridad Designada
del Sistema Portuario Nacional

Registro y Control de acceso peatonal.
Detectores de metales para inspección no intrusiva.
Alcoholimetro y rayos X para equipaje.
Inspección física ingreso y egreso de la Instalación Portuaria.

Autoridad Designada
del Sistema Portuario Nacional

Decreto número 26-2024 del Congreso de la República de Guatemala, artículo 6, que establece:

"*...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*."

PUERTOS DE GUATEMALA

Guatemala cuenta con tres puertos marítimos distribuidos entre ambas costas: Santo Tomás de Castilla y Puerto Barrios en el litoral Caribe, y Puerto Quetzal en el litoral Pacífico; este último es un puerto multipropósito que cuenta con 5 terminales especializadas en su interior y existen 3 terminales especializadas de Graneles Líquidos en la jurisdicción de San José, Escuintla.

Puerto Quetzal es operado por Empresa Portuaria Quetzal y Puerto Santo Tomás de Castilla por Empresa Portuaria Nacional Santo Tomás de Castilla, es decir que son operados por el Estado. Puerto Barrios, la propiedad es estatal, pero es operada por la empresa privada Chiquita Guatemala. Estos operadores estatales y operador privado gestionan la infraestructura, superestructura, servicios y administración portuaria.

Puertos, Terminales Especializadas y Operadores de Servicios Portuarios afectos al cumplimiento del Código PBIP

Litoral Pacífico

5 Terminales Especializadas

15 Operadores de Servicios Portuarios

Graneles Líquidos
en San José, Escuintla

3 Terminales Especializadas

Litoral Atlántico

Puerto Santo Tomás de Castilla

19 Operadores de Servicios Portuarios

Terminal Ferroviaria Puerto Barrios

Además de los puertos, también se controlan las Terminales Especializadas y los Operadores de Servicios Portuarios. Estos últimos no cuentan con muelles propios, ya que operan a través de los muelles de Puerto Quetzal y Puerto Santo Tomás de Castilla.

3 Puertos

8 Terminales Especializadas

34 Operadores de Servicios Portuarios

45

Instalaciones afectas al Código PBIP

01

Introducción

Introducción

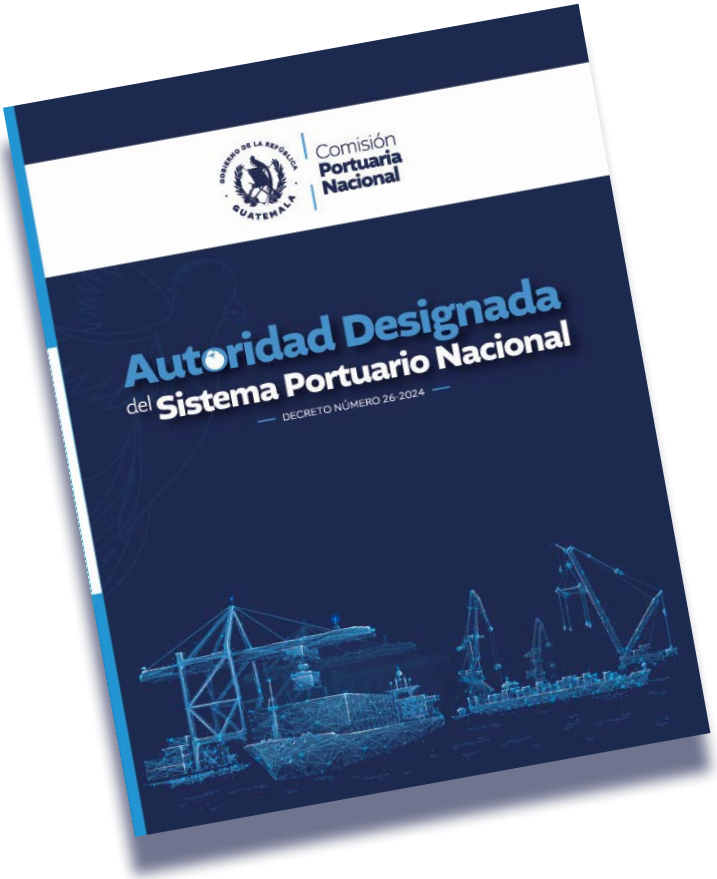
La Autoridad Designada del Sistema Portuario Nacional -ADSPN-, por designación expresa del Estado de Guatemala, es el órgano técnico competente para velar por el cumplimiento de las regulaciones en materia de protección, asesoría y capacitación portuaria en el Sistema Portuario Nacional, para ello mantiene coordinaciones y adopta las directrices de organismos internacionales tales como la Organización de Estados Americanos (OEA), Organización Marítima Internacional (OMI), Foro PBIP Internacional, Comité Interamericano Contra el Terrorismo (CICTE-OEA) y también mantiene relación con otras Autoridades Designadas de la región encargadas de la protección portuaria contenida en el Código Internacional para la Protección de Buques y de las Instalaciones Portuarias (Código PBIP); promoviendo así el desarrollo de los puertos, basados en esquemas de alto cumplimiento de las medidas de protección portuaria, brindando a la Alta Dirección de las entidades afectas al cumplimiento de las medidas y a los Oficiales de las Instalaciones Portuarias (OPIP) formación, asistencia técnica y fortalecimiento de capacidades en general.

Con base a las facultades legales otorgadas a la entidad del y bajo una "Visión País" de modernización portuaria plasmada en la meta Puertos del Sistema de Metas dela Presidencia de la República de Guatemala, se articulan esfuerzos y coordinaciones a efecto de 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

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 robustezcan sus sistemas y medidas de protección portuaria, con enfoque basado en riesgo, continuidad operativa, integridad de la información y mejora continua, a efecto de elevar el nivel de cumplimiento del Código PBIP, Parte A, secciones 15.5, 16.3 y 17.2.12, Parte B,
secciones 16.49 a 16.53; Decreto Número 26-2024 del Congreso de la República de Guatemala, 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, Reglamento para la Protección de los Buques e Instalaciones Portuarias, 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 y lineamientos técnicos para que la Alta Dirección y los OPIP adopten tecnologías para robustecer los procesos que contemplan en sus Planes de Protección de sus Instalaciones Portuarias (PPIP) considerando los siguientes:

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

03

Tecnologías para la Protección Portuaria

Tecnologías para la Protección Portuaria

El presente capítulo detalla la diversidad de tecnologías que pueden aplicarse a cada una para protección, tales como **equipos, barreras y dispositivos para su aplicación y robustecimiento de la protección en las instalaciones portuarias**. Tiene como propósito establecer el **marco conceptual y metodológico** que permitirá analizar, describir y clasificar los distintos equipos, barreras y tecnologías aplicables a la protección de las instalaciones portuarias. Este apartado introduce los criterios de análisis que se emplearán a lo largo de la guía, explica la lógica de clasificación funcional adoptada y orienta al lector sobre la estructura y el contenido que se desarrollarán en los apartados subsecuentes.

El enfoque planteado no evalúa, categoriza o define el resultado del uso de cada tecnología, sino que las examina con base en **la función específica que desempeñan dentro de un sistema integral de protección**, considerando su contribución al fortalecimiento del sistema integral de protección de una instalación, es decir, cómo cada tecnología puede contribuir a conformar un ecosistema de protección, y no que se invierta en tecnologías dispersas y no contactadas. Ver anexo No.1

Para efectos de esta guía, la protección de las instalaciones portuarias se concibe como un **sistema integrado y escalonado**, compuesto por diversos medios técnicos, físicos y operativos que actúan de manera complementaria. Bajo este enfoque, ningún equipo, barrera o tecnología resulta suficiente por sí sola para garantizar un nivel adecuado de protección.

A. Clasificación funcional de tecnologías por tipo de uso

Para homogenizar el análisis y facilitar la comparación entre distintos medios de protección, esta Guía adopta una clasificación funcional basada en cuatro funciones fundamentales, identificadas mediante los códigos D1, D2, D3 y R1.

Estas funciones representan las distintas etapas y capacidades que pueden aportar los equipos, barreras y tecnologías dentro del sistema de protección portuaria.

D1 – Detección
La función de Detección corresponde a la capacidad **de identificar, descubrir o generar alertas oportunas** relacionadas con la presencia de amenazas, anomalías o eventos relevantes para la seguridad.

D2 – Disuasión
La función de disuasión se refiere a la capacidad de **prevenir o inhibir acciones no autorizadas** mediante la percepción de vigilancia, la presencia visible de medios de protección o la emisión de advertencias explícitas.

D3 – Demorar
La función de demora consiste en la capacidad de **retardar el avance, acceso o acción de una amenaza**, incrementando el tiempo disponible para la activación de medidas de respuesta.

R1 – Reacción
La función de Reacción hace referencia a las **acciones posteriores a la detección de un evento**, orientadas a controlar, contener o mitigar sus efectos.

B. Interpretación del esquema visual de clasificación

El esquema gráfico que acompaña este marco conceptual utiliza colores como referencia visual, sin que estos impliquen una clasificación automática de los equipos o tecnologías.

Es importante señalar que las funciones asignadas no determinan por sí mismas que una tecnología sea efectiva o no efectiva. Un mismo equipo puede contribuir simultáneamente a varias funciones, y su valor dependerá de su correcta aplicación, configuración e integración dentro del sistema de protección.

Color verde: identifica funciones de carácter predominantemente del equipo, barrera o tecnología que pueden ser aprovechadas al 100%.

Detección -D1-	Disuación -D2-	Demora -D3-	**Reacción -R1-**

Color rojo: identifica funciones que no pueden ser aprovechadas al 100% por el tipo de equipo, barrera o tecnología.

Detección -D1-	Disuación -D2-	**Demora -D3-**	Reacción -R1-

3.1 Tecnologías Aplicables a la Protección Portuaria

3.1.1 Sistemas no tripulados (Aéreos y acuáticos)

Los Sistemas No Tripulados aéreos y acuáticos fortalecen la protección portuaria al facilitar la vigilancia y detección de amenazas en áreas terrestres y acuáticas críticas y de difícil acceso. Conforme al Código PBIP, estas tecnologías apoyan la evaluación permanente de riesgos y la prevención de actos ilícitos, reforzando la defensa en profundidad. Su implementación contribuye a mantener niveles adecuados de protección y a una respuesta oportuna por parte del OPIP y la Autoridad Portuaria.

Tecnología	Tipos existentes	Funcionalidad	Complementos / Accesorios para robustecer su uso	Ilustración
Dron aéreo (UAV)	**Multirrotor:** despegue vertical, ideal para vigilancia puntual y seguimiento. (imagen 1) **Ala fija:** mayor autonomía y cobertura, usada para patrullajes extensos. (Imagen 2)	Vehículo aéreo no tripulado utilizado para vigilancia, patrullaje y evaluación de incidentes.	• Cámaras térmicas e infrarrojas • Cámaras de alta resolución y zoom óptico • Sensores LiDAR • Altavoces y sirenas • Reflectores LED nocturnos • Módulos RTK/GPS de alta precisión • Paracaídas de seguridad • Enlaces de comunicación de largo alcance	 D1 D2 D3 R1 D1 D2 D3 R1
Dron acuático de superficie (USV)	**Patrullaje:** recorrido autónomo del espejo de agua. (Imagen 3) **Vigilancia costera:** monitoreo continuo del límite marítimo-portuario. (Imagen 4)	Vehículo no tripulado que opera sobre el agua para monitoreo marítimo.	• Radar de corto alcance • Cámaras giroestabilizadas día/noche • Sensores meteorológicos y oceanográficos • Sonar de barrido lateral • Sistemas AIS (identificación de embarcaciones) • Altavoces para advertencia acústica· Enlaces satelitales o 4G/5G	 D1 D2 D3 R1 D1 D2 D3 R1
Dron subacuático (UUV)	**Inspección de cascos:** búsqueda de objetos adheridos. (Imagen 5) **Inspección de fondo:** detección de anomalías subacuáticas. (Imagen 6)	Vehículo no tripulado para operaciones bajo el agua.	• Sonar multihaz o de imágenes • Cámaras de baja luminosidad • Brazo robótico para manipulación • Luces LED subacuáticas • Sensores de profundidad y corriente • Sistemas de posicionamiento USBL/LBL • Cables umbilicales reforzados	 D1 D2 D3 R1 D1 D2 D3 R1

Tecnología	Tipos existentes	Funcionalidad	Complementos / Accesorios para robustecer su uso	Ilustración
Estación de drones (Drone Dock)	**Fija:** instalada permanentemente. (Imagen 7) **Móvil:** reubicable según operación. **Autónoma:** recarga, despliegue y resguardo automático. (Imagen 8)	Plataforma que permite carga, resguardo y operación autónoma de drones.	• Sistemas de recarga rápida o inalámbrica • Paneles solares • Climatización y sellado IP para intemperie • Sistemas anti-interferencia y ciberseguridad • Software de gestión de flotas • Integración con centros de control (C2) • Cámaras de monitoreo de la estación	D1 D2 D3 R1 D1 D2 D3 R1

3.1.2 Cámaras de videovigilancia(Fijas, portátiles y corporales)

Las cámaras de videovigilancia fijas y corporales constituyen un elemento esencial para la protección de las instalaciones portuarias, al permitir el monitoreo continuo, la disuasión y el registro de actividades en áreas sensibles. En concordancia con el Código PBIP, estas tecnologías apoyan la detección temprana de incidentes, la verificación de accesos y la recolección de evidencias. Su uso fortalece la supervisión operativa y la capacidad de respuesta del personal de protección en los distintos niveles de seguridad.

Tecnología	Tipos existentes (con definición)	Funcionalidad	Complementos / Accesorios para ampliar su uso	Ilustración
Cámaras CCTV	**Fijas:** monitoreo constante de un área. (Imagen 09) **PTZ:** giro, inclinación y zoom controlados remotamente. (Imagen 10)	Vigilancia continua de espacios mediante video en circuito cerrado para supervisión y registro de eventos.	• Lentes intercambiables (gran angular, teleobjetivo) • Iluminadores infrarrojos (IR) • Carcasas antivandálicas y climatizadas • Joysticks de control PTZ • Integración con centros de monitoreo	 D1 D2 D3 R1 D1 D2 D3 R1
Cámaras térmicas	**Fijas:** detección permanente de fuentes de calor. (Imagen 11) **PTZ:** seguimiento térmico dinámico de objetivos. (Imagen 12)	Detección de personas, vehículos o focos de calor en condiciones de baja o nula visibilidad.	• Software de análisis térmico • Fusión térmica + visible • Alarmas automáticas por umbrales de temperatura • Calibradores térmicos • Integración con sistemas perimetrales • Carcasas para exteriores extremos	 D1 D2 D3 R1 D1 D2 D3 R1

Tecnología	Tipos existentes (con definición)	Funcionalidad	Complementos / Accesorios para ampliar su uso	Ilustración
Cámaras con analítica de video	**Intrusión:** detección de acceso no autorizado. (Imagen 13) **Objetos:** detección de abandono o retiro. (Imagen 13) **Comportamiento:** análisis de patrones anómalos. (Imagen 13)	Análisis automatizado del video para generar alertas y eventos sin intervención humana constante.	• Motores de inteligencia artificial • Servidores de procesamiento (GPU) • Licencias de analítica avanzada • Integración con control de accesos y alarmas • Dashboards de visualización de eventos • Sistemas de notificación en tiempo real	 D1 D2 D3 R1
Cámaras 360°	**Panorámicas**: cobertura total del entorno sin puntos ciegos. (Imagen 14)	Vigilancia integral de áreas amplias con una sola cámara.	• Software de dewarping (corrección de imagen) • Analítica multi-zona • Soportes especiales de montaje • Integración con VMS centralizado	 D1 D2 D3 R1
Cámaras corporales	**Pecho:** control de inspecciones y procedimientos. (Imagen 15) **Casco:** uso en operaciones tácticas o técnicas. (Imagen 16)	Registro audiovisual portátil de las actividades del personal en campo.	• Docking stations de carga y descarga • Software de gestión de evidencias • GPS integrado· Botón de evento o emergencia • Micrófonos con reducción de ruido	 D1 D2 D3 R1 D1 D2 D3 R1
Cámaras anti-explosión	**ATEX Zona 1:** riesgo permanente de atmósferas explosivas. (Imagen 17) **ATEX Zona 2**: riesgo ocasional. (Imagen 17)	Vigilancia en entornos industriales con presencia de gases, vapores o polvo inflamable.	• Carcasas certificadas ATEX • Sistemas de purga y presurización • Cableado y conectores anti-chispa • Iluminación certificada ATEX • Integración con sistemas industriales (SCADA) • Monitoreo remoto seguro	 D1 D2 D3 R1
Cámaras subacuáticas	**Fijas:** monitoreo continuo bajo el agua. (Imagen 18)	Vigilancia e inspección visual en entornos subacuáticos.	• Iluminación LED subacuática • Carcasas de alta presión • Sistemas de limpieza automática de lente • Cableado subacuático reforzado • Monitores y grabadores especializados	 D1 D2 D3 R1

3.1.3 Sistemas de control de acceso (Biométricos, cámaras y barreras)

Los **sistemas de control de acceso biométricos y mediante barreras** son fundamentales para regular y restringir el ingreso de personas, vehículos y bienes a las instalaciones portuarias. En alineación con el **Código PBIP**, estas tecnologías garantizan que solo personal autorizado acceda a zonas restringidas, reduciendo el riesgo de intrusiones y actos ilícitos. Su aplicación refuerza la trazabilidad, la disuasión y el cumplimiento de los niveles de protección establecidos.

Tecnología	Tipos existentes	Funcionalidad	Complementos / Accesorios para robustecer su uso	Ilustración
Reconocimiento de placas (LPR)	**Fijo:** carriles controlados. (Imagen 19) **Móvil:** patrullaje o puntos temporales. (Imagen 19)	Identificación automática de matrículas vehiculares para control, registro y seguridad.	• Iluminación infrarroja • Software analítico • Enlace con barreras vehiculares	 D1 D2 D3 R1
Cámaras OCR (OCR)	**OCR especializado:** documentos, placas o etiquetas. (imagen 20)	Captura y reconocimiento óptico de caracteres para automatizar registros e identificación visual.	Cámaras HD, iluminación dedicada, software OCR, integración con LPR, ACS y bases de datos.	 D1 D2 D3 R1
Biometría (BIO)	**Huella:** contacto físico. (Imagen 21) **Rostro:** sin contacto, alta fluidez. (Imagen 22) **Iris:** alta seguridad. (Imagen 23)	Identificación de usuarios mediante rasgos físicos únicos, reduciendo suplantaciones.	Cámaras biométricas, lectores multisensor, bases de datos, integración con sistemas ACS.	 D1 D2 D3 R1
Torniquetes (Smart Turnstile)	**Medio cuerpo:** control básico. (Imagen 24) **Cuerpo completo:** máxima restricción. (Imagen 25)	Barreras automatizadas que regulan y ordenan el paso peatonal en accesos controlados.	Lectores RFID o biométricos, sensores anti-passback, contadores de personas, señalización LED.	 D1 D2 D3 R1
Barreras vehiculares (Vehicle Barrier)	**Hidráulicas:** alta resistencia. (Imagen 26) **Electromecánicas:** uso continuo. (Imagen 27)	Control físico del ingreso y salida de vehículos, reforzando la seguridad perimetral.	Lazos magnéticos, LPR, controles remotos, semáforos, botones de emergencia.	 D1 D2 D3 R1
RFID de corto alcance (RFID)	**HF / UHF pasivo:** lectura cercana. (Imagen 28) **Tarjetas y tags:** identificación personal o vehicular. (Imagen 29)	Identificación mediante radiofrecuencia a corta distancia, permitiendo accesos rápidos y controlados.	Lectores RFID, antenas, tarjetas o tags, software de control, integración con ACS, torniquetes y barreras.	 D1 D2 D3 R1

3.1.4 Sistemas de detección e intrusión

Los sistemas de detección e intrusión permiten identificar accesos no autorizados, movimientos sospechosos o intentos de violación del perímetro en las instalaciones portuarias mediante sensores, alarmas y tecnologías especializadas. En conformidad con el Código PBIP, estos sistemas apoyan la detección temprana de amenazas y la activación oportuna de los procedimientos de respuesta. Su implementación fortalece la vigilancia preventiva y contribuye al mantenimiento de los niveles de protección establecidos.

Tecnología	Tipos existentes	Funcionalidad	Complementos / Accesorios para robustecer su uso	Ilustración
Cercas inteligentes (IDS Fence)	**Vibración:** detecta cortes o escalamiento. (Imagen 30) **Microfibra:** alta sensibilidad perimetral. (Imagen 31)	Sistema de detección perimetral que identifica intentos de intrusión física en cercas.	Centrales de alarma, software de monitoreo, CCTV, integración con iluminación y notificación remota	 D1 D2 **D3** R1 D1 D2 D3 R1
Sensores infrarrojos (IR Sensor)	**Activos:** emisor–receptor. Pasivos: detección de calor corporal. (Imagen 32)	Detección de movimiento o presencia mediante interrupción de haces o variación térmica.	Torres de sensores, cámaras PTZ asociadas, centrales de alarma, sistemas de monitoreo perimetral.	 D1 D2 **D3** R1
Sensores de microondas (Microwave Sensor)	**Perimetrales:** cobertura de grandes distancias. (Imagen 33)	Detección de intrusión mediante ondas electromagnéticas que crean un campo de protección.	Postes de instalación, software de análisis, integración con CCTV y alarmas perimetrales.	 D1 D2 **D3** R1
Sensores subacuáticos (UW Sensor)	**Fijos:** protección de perímetros. (Imagen 34)	Detección de intrusión acuática en zonas sumergidas o cuerpos de agua.	Sonares, sistemas de monitoreo acuático, integración con centros de control y alertas.	 D1 D2 **D3** R1

3.1.5 Sistemas de inspección no intrusiva

Los sistemas de inspección no intrusiva permiten la revisión de personas, vehículos, carga y contenedores sin necesidad de apertura física, mediante el uso de tecnologías como rayos X, escáneres y detectores especializados. En alineación con el Código PBIP, estos sistemas fortalecen la detección de objetos, materiales o amenazas ocultas, reduciendo riesgos y aumentando la eficiencia operativa. Su aplicación contribuye a prevenir actos ilícitos y a mantener los niveles de protección establecidos en las instalaciones portuarias.

Tecnología	Tipos existentes	Funcionalidad	Complementos / Accesorios para robustecer su uso	Ilustración
Rayos X de carga (X-Ray Cargo)	**Fijos:** patios y accesos. (Imagen 35) **Móviles:** inspección aleatoria. (Imagen 36)	Inspección interna y no intrusiva de carga para detección de amenazas, contrabando o anomalías.	Software de análisis de imágenes, bases de datos de perfiles, integración con OCR y LPR, centros de monitoreo.	 D1 D2 D3 R1 D1 D2 D3 R1
Rayos X portátiles (PX-Ray)	**Panel plano:** inspección de maletas. (Imagen 37)	Inspección portátil y flexible de equipaje u objetos sospechosos en campo.	Baterías extendidas, estaciones de carga, monitores remotos, software de visualización.	 D1 D2 D3 R1
Biometría (BIO)	**Arco:** inspección de personas. (Imagen 38) **Manual:** inspección focalizada. (Imagen 39)	Identificación de objetos metálicos ocultos en personas o pertenencias.	Sensibilidad ajustable, alarmas sonoras y visuales, integración con torniquetes y control de accesos.	 D1 D2 D3 R1 D1 D2 D3 R1

3.1.6 Sistemas de sellado y trazabilidad

Los sistemas de sellado y trazabilidad permiten asegurar la integridad de la carga, contenedores y unidades logísticas mediante sellos físicos o electrónicos, así como el seguimiento de su desplazamiento a lo largo de la cadena portuaria. En concordancia con el Código PBIP, estas soluciones tecnológicas contribuyen a prevenir manipulaciones no autorizadas, mejorar la identificación de riesgos y fortalecer la confianza en las operaciones marítimo-portuarias. Su implementación refuerza el control, la transparencia y la detección temprana de posibles actos ilícitos.

Tecnología	Tipos existentes	Funcionalidad	Complementos / Accesorios para robustecer su uso	Ilustración
Marchamos electrónicos (E-Seal)	**RFID:** detección de apertura. (Imagen 40) **GPS:** seguimiento en ruta. (Imagen 41) **Satelital:** cobertura remota. (Imagen 41)	Control electrónico de la integridad de la carga, detectando aperturas no autorizadas y eventos en tránsito.	Plataformas de monitoreo, alertas en tiempo real, integración con GPS y centros de control logístico.	D1 D2 D3 R1 D1 D2 D3 R1
RFID (RFID)	**Activo:** largo alcance. (Imagen 42)	Identificación y trazabilidad mediante radiofrecuencia, aplicada a carga, activos o contenedores.	Lectores RFID fijos y móviles, antenas, software de gestión e integración con plataformas reconocidas.	D1 D2 D3 R1
Sellos GPS	**Tiempo real:** monitoreo continuo. (Imagen 43)	Seguimiento de la carga en tiempo real, con registro de ubicación y eventos durante el transporte.	Plataforma GPS, comunicaciones celulares o satelitales, alertas geocercas e integración con plataformas reconocidas.	D1 D2 D3 R1

3.1.7 Sistemas de disuasión (Analítica, predicción y reacción)

Los sistemas de disuasión tienen como finalidad prevenir actos ilícitos mediante la presencia visible de tecnologías y dispositivos que reducen la intención de intrusión o interferencia en las instalaciones portuarias. En concordancia con el Código PBIP, estos sistemas fortalecen la protección preventiva al generar un efecto psicológico disuasivo frente a potenciales amenazas. Su aplicación contribuye a mantener el orden, reforzar la percepción de seguridad y apoyar los niveles de protección establecidos.

Tecnología	Tipos existentes	Funcionalidad	Complementos / Accesorios para robustecer su uso	Ilustración
Iluminación disuasiva (D-Light)	**Perimetral:** cercas y accesos. (Imagen 44) **Activada por movimiento:** encendido automático. (Imagen 45) **Iluminación automatizada:** horarios programados. (Imagen 45)	Uso estratégico de iluminación intensa para disuadir intrusos y aumentar la visibilidad	Sensores de movimiento, integración con CCTV, temporizadores, respaldo energético.	 D1 D2 D3 R1
Señalización disuasiva (Warning Signage)	**Física:** letreros visibles. (Imagen 46) **Digital:** pantallas informativas. (Imagen 47)	Advertencia visual de zonas protegidas, monitoreadas o restringidas.	Señalización reflectiva, integración con sistemas de seguridad, normativas legales visibles.	 D1 D2 D3 R1
Sirenas y alarmas sonoras (Audio Alarm)	**Locales:** activación puntual. (Imagen 48) **Centralizadas:** red de alarmas. (Imagen 49) **Audio ambiental:** sonidos simulados. (Imagen 49)	Emisión de señales acústicas para alertar y disuadir ante eventos sospechosos.	Paneles de alarma, sensores perimetrales, baterías de respaldo, notificaciones remotas.	 D1 D2 D3 R1
Sistemas de audio disuasivo (PA / Voice Alarm)	**Mensajes pregrabados:** advertencia automática. (Imagen 50) **En vivo:** control desde central. (Imagen 50)	Emisión de mensajes de advertencia para disuadir intrusiones o conductas no autorizadas.	Altavoces perimetrales, integración con sensores y CCTV, software de gestión de audio.	 D1 D2 D3 R1
Disuasión visual avanzada (Strobe / Flash)	**Luces estroboscópicas:** alta intensidad. (Imagen 51) **Balizas:** señalización intermitente. (Imagen 52)	Impacto visual inmediato para disuadir y llamar la atención ante eventos de riesgo.	Integración con alarmas, sensores de intrusión, controladores de iluminación.	 D1 D2 D3 R1

3.1.8 Software (Administración, analítica, predicción y reacción)

Los sistemas de software para la administración, analítica, predicción y reacción integran y gestionan la información proveniente de los distintos sistemas de protección portuaria, permitiendo una visión unificada y en tiempo real de la seguridad de la instalación. En correspondencia con el Código PBIP, estas plataformas facilitan el análisis de datos, la identificación de patrones de riesgo y la anticipación de amenazas, apoyando la toma de decisiones informadas. Su uso fortalece la capacidad de respuesta ante incidentes y contribuye al mantenimiento eficiente de los niveles de protección establecidos.

Tecnología	Tipos existentes	Funcionalidad	Complementos / Accesorios para robustecer su uso	Ilustración
Plataforma de gestión de seguridad (PSIM)	**Centralizada:** múltiples sistemas. (Imagen 53) **Distribuida:** operación por sitios. (Imagen 53)	Administración integral de eventos, alarmas y respuestas desde una sola plataforma.	Integración con CCTV, ACS, LPR, sensores perimetrales, mapas GIS.	 D1 D2 D3 R1
Sistema de gestión de video (VMS)	**Monitoreo en vivo:** vigilancia continua. (Imagen 54) **Forense:** búsqueda y análisis histórico. (Imagen 54)	Administración y análisis inteligente de video para detección y verificación de eventos.	Analítica de video, IA, almacenamiento escalable, integración con PSIM.	 D1 D2 D3 R1
Analítica avanzada e IA (AI Analytics)	**Comportamiento:** patrones anómalos. (Imagen 55) **Objetos:** personas, vehículos, objetos. (Imagen 55)	Análisis automático de datos para detección temprana y reducción de falsas alarma.	Modelos de IA, GPU, integración con VMS, sensores y bases de datos.	 D1 D2 D3 R1
Software de predicción y riesgo (Predictive Analytics)	**Tendencias:** análisis histórico. (Imagen 56) **Escenarios:** simulación de eventos. (Imagen 56)	Predicción de riesgos y anticipación de incidentes mediante análisis estadístico y modelos predictivos.	Big Data, IA, integración con fuentes operativas y sistemas históricos.	 D1 D2 D3 R1
Centro de comando y control (C2 / C4)	**Táctico:** operación inmediata. (Imagen 57) **Estratégico:** toma de decisiones. (Imagen 57)	Consolidación de información para dirección, coordinación y control operativo.	Videowalls, PSIM, GIS, comunicaciones críticas, sistemas de reporte.	 D1 D2 D3 R1
Software de reportes e inteligencia operativa (BI Security)	**Operativo:** reportes diarios. (Imagen 58) **Ejecutivo:** indicadores estratégicos. (Imagen 58)	Transformación de datos en indicadores, métricas y KPIs para toma de decisiones.	Dashboards, herramientas BI, exportación a PDF/Excel, integración multisistema.	 D1 D2 D3 R1

04

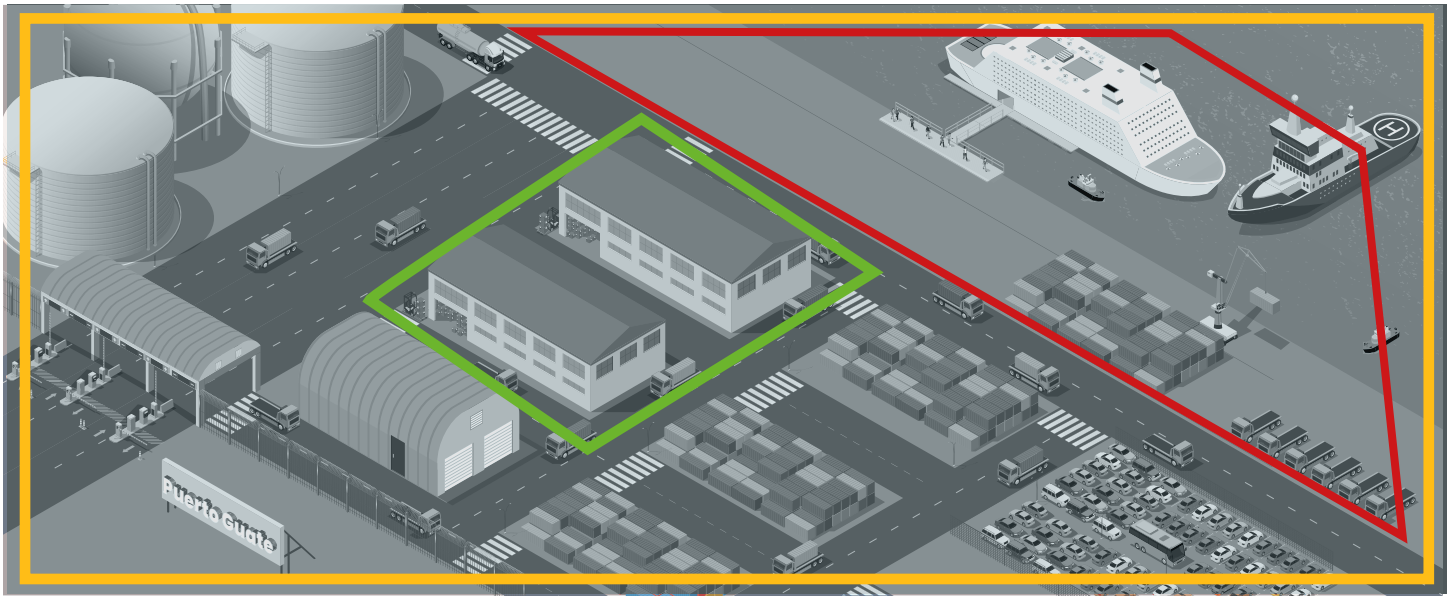
Modelo de Anillos para Proteger la Instalación Portuaria

Modelo de Anillos para Proteger la Instalación Portuaria

4.1 Orientación Técnica de Tecnologías

Para abordar los sucesos, amenazas y fallos en la protección que enfrentan actualmente las instalaciones portuarias de Guatemala, es necesario adoptar medidas de prevención, reacción y mitigación frente a la diversidad de riesgos existentes. En este contexto, la tecnología desempeña un papel clave, ya que permite reducir riesgos asociados a amenazas, fallas humanas y deficiencias en la comunicación, además de optimizar tiempos y costos. Esta Guía presenta el resultado de la identificación de mejores prácticas y de la aplicación de diversas tecnologías a nivel global en instalaciones portuarias, y considerando un modelo concéntrico de anillos, se propone una integración de tecnologías en cada anillo para asegurar la instalación.

4.2 Modelo de Anillos de Protección



Anillo **1** Anillo **2** Anillo **3**

Las tecnologías descritas adquieren su máximo valor para robustecer la protección portuaria cuando se organizan estratégicamente bajo un modelo de defensa.

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 sistemas de detección de intrusos en el perímetro, 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, aquí se busca que toda persona, vehículo y carga sea controlada o sometida a estos controles previo a su ingreso a la instalación; también se busca que no se den operaciones sospechosas dentro de la instalación portuaria.

B. Anillo 2 — Áreas operacionales

Objetivo:
Controlar y rastrear el flujo y la permanencia 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 y que acceda únicamente a las áreas a las que le fue autorizado el ingreso.

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 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 de la instalación portuaria, de modo que cualquier discrepancia entre lo declarado y lo verificado genere una alerta automática.

C. Anillo 3 — Áreas o activos críticos

Objetivo:
Proteger las áreas, infraestructura y sistemas críticos, de mayor valor estratégico de la instalación.

Este anillo aplica los controles más estrictos sobre los activos cuya afectación comprometería directamente la operatividad de la instalación 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, por eso se buscan ecosistemas de protección.

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.

Autoridad Designada
del Sistema Portuario Nacional

ZIM
ZCSU 4008484
ZCSU 4015267
JXLU 4010970
Hapag-Lloyd
HLBU 807286 6
45U1
STEEL FLOOR
CROWLEY

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.

4.3 Matriz de Tecnologías Avanzadas

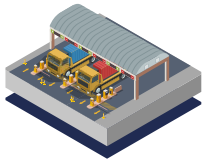
Soluciones Integradas por Función de Defensa y Anillo de Seguridad

	ANILLO 1 Perímetro	**ANILLO 2** Operacional	**ANILLO 3** Activos Críticos
Disuadir	· Iluminación disuasiva · Señalización física y digital · Sirenas y alarmas sonoras	· Cámaras corporales (visibilidad operativa) · Cámaras anti-explosión (zonas industriales · Cámaras subacuáticas (entornos críticos)	· Señalización de áreas restringidas · Políticas de control y trazabilidad de carga
Detectar	· Cámaras CCTV fijas/PTZ · Cámaras térmicas · Cámaras 360° · Cámaras con analítica de video · Cercas inteligentes · Sensores infrarrojos · Sensores microondas · Sensores subacuáticos	· Reconocimiento de placas (LPR) · Cámaras OCR · Biometría (huella, rostro, iris) · RFID corto alcance · Rayos X de carga y portátiles · Detectores de metales	· Marchamos electrónicos · Sellos GPS · RFID activo de largo alcance
Demorar	· Torniquetes inteligentes · Barreras vehiculares	· Puertas reforzadas · Compartimentación de áreas	· Controles de acceso con biometría avanzada · Protocolos de trazabilidad reforzada
Responder	· Cámaras PTZ auto-tracking · Drones aéreos (UAV) · Drones acuáticos (USV) · Drones subacuáticos (UUV) · Estaciones de drones	· Unidades móviles de respuesta · Sistemas de notificación y monitoreo en tiempo real	· Supresión automática de incidentes · Integración con centros de control logístico

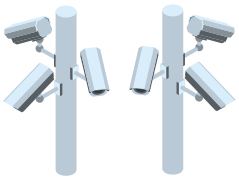
4.3.1 Anillo 1 – Perímetro de la Instalación Portuaria

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.

ALCANCE DE PROCESO
1. ACCESO A LA INSTALACIÓN PORTUARIA
2. VIGILANCIA DE PROTECCIÓN DE LA INSTALACIÓN PORTUARIA



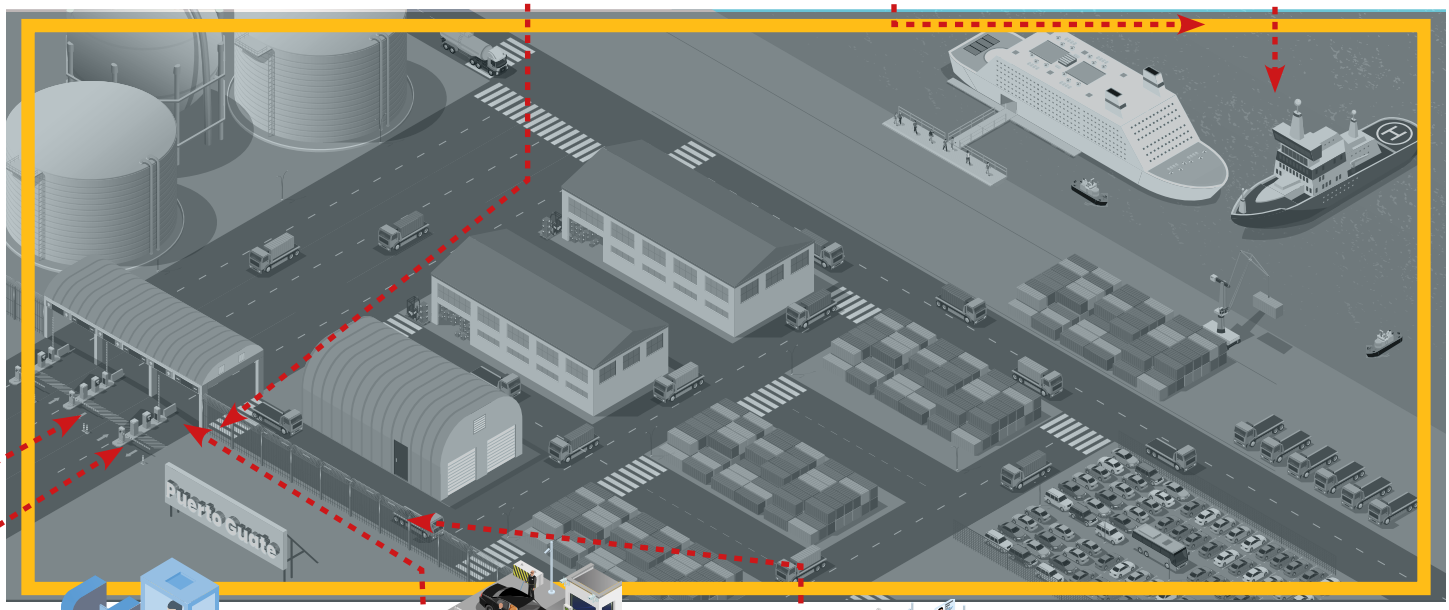
Acceso transporte pesado:
1. Biométricos
2. RFID
3. Cámaras fijas y PTZ
4. Cámaras LPR y OCR
5. Barreras
6. Rayos X portátil



Perímetro:
1. Iluminación fija y automática
2. Altavoces de alertas

Vigilancia Perímetro Cámaras
1. Fijas
2. PTZ
3. Térmicas
4. Drones aéreo
5. Cámaras corporales

Canal de acceso y dársena de maniobras:
1. Dron acuático
2. Dron Subacuático



Acceso peatonal:
1. Biométricos
2. Rayos X
3. Arco detector
4. Detector Manual
5. Cámaras fijas y PTZ

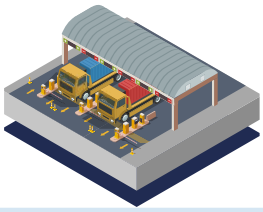
Acceso vehículos livianos
1. Biométricos
2. Cámaras fijas y PTZ
3. Rayos X portátil
4. RFID
5. Cámara LPR
6. Barreras

Muros vivos: Sensores
1. Vibración
2. Infrarrojos
3. Microondas
4. Fibra
5. Subacuáticos

4.3.2 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.

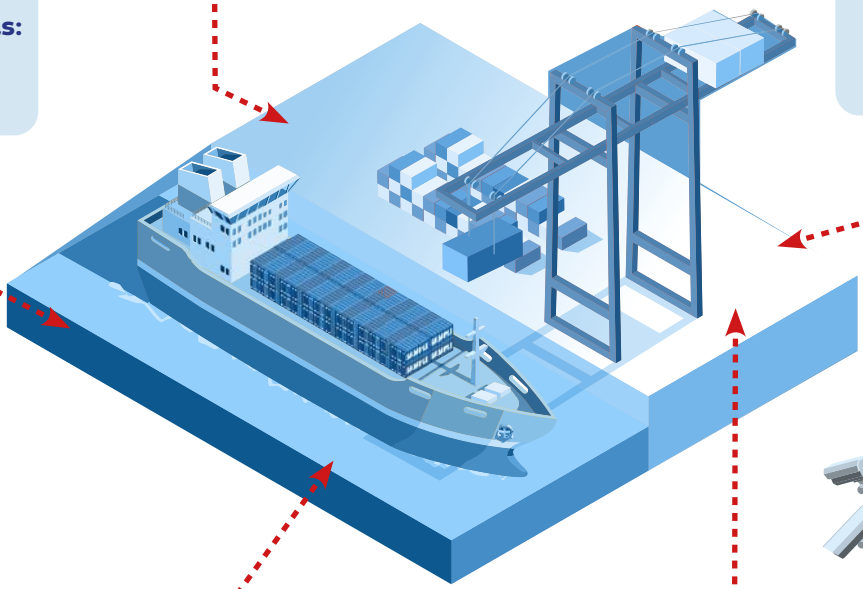
ALCANCE DE PROCESO
1. INTERFAZ BUQUE-PUERTO
2. MANIPULACIÓN DE LA CARGA



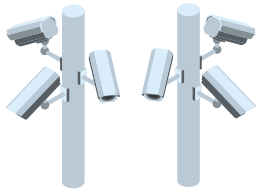
Acceso transporte pesado:
1. RFID
2. Rayos X para carga
3. Geocercas
4. Marchamos electrónicos

Vigilancia
Canal de acceso y dársena de maniobras:
1. Dron acuático
2. Dron Subacuático

Perímetro interfaz buque-puerto:
1. Iluminación fija y automática
2. Altavoces de alertas



Sensores:
1. Subacuáticos



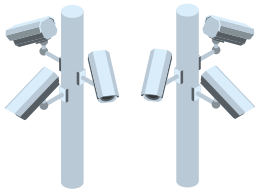
Vigilancia/Cámaras:
1. Fijas
2. PTZ
3. Térmicas
4. Drones aéreos

4.3.3 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.

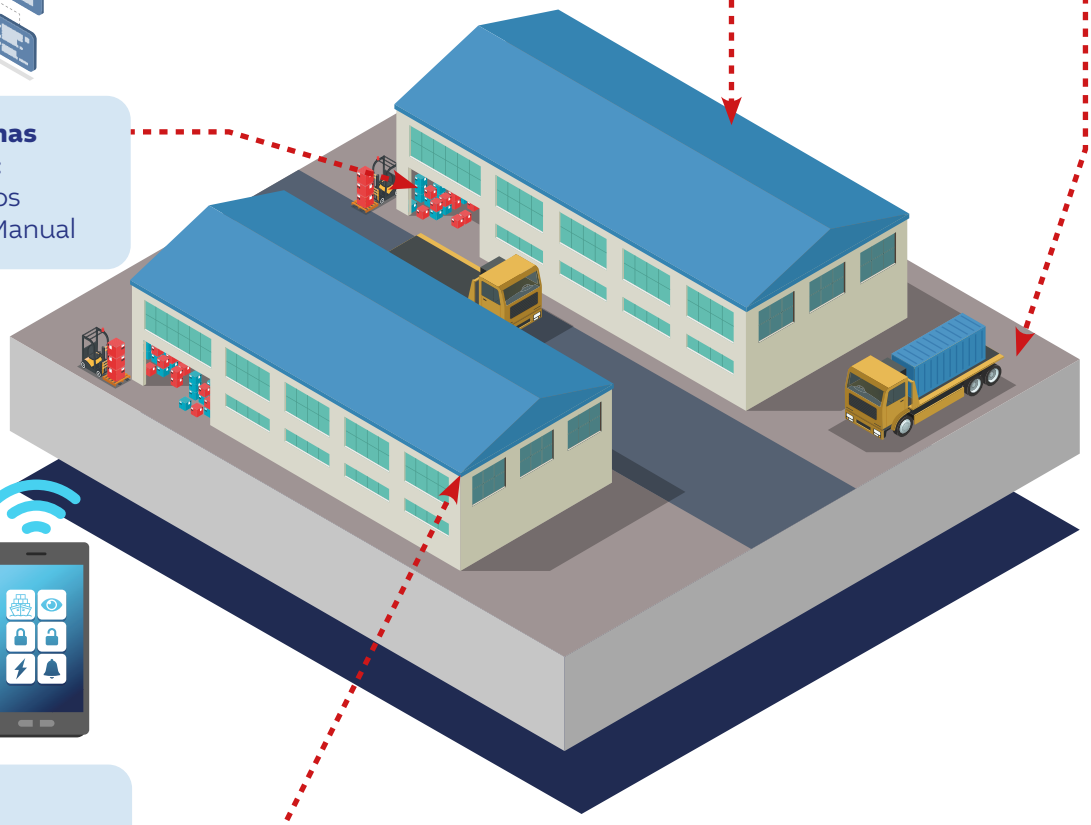
ÀLCANCE DE PROCESO
1. ZONAS RESTRINGIDAS



Vigilancia Perímetro Cámaras:
1. Fijas
2. PTZ
3. Térmicas

Perímetro:
1. Iluminación fija y automática
2. Altavoces de alertas

Acceso a zonas restringidas:
1. Biométricos
2. Detector Manual



Sensores:
1. Infrarrojos
2. Microondas

TRITON
Touax
33
CSC 340
Seacastle
45

05

Registro, Integración y Uso de la Información Generada

Información Generada

La información generada por los sistemas tecnológicos o ecosistemas de Protección Portuaria 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 que los controles están activos y operativos, complementando la documentación formal del Plan de Protección de la Instalación Portuaria.

F. Interoperabilidad institucional

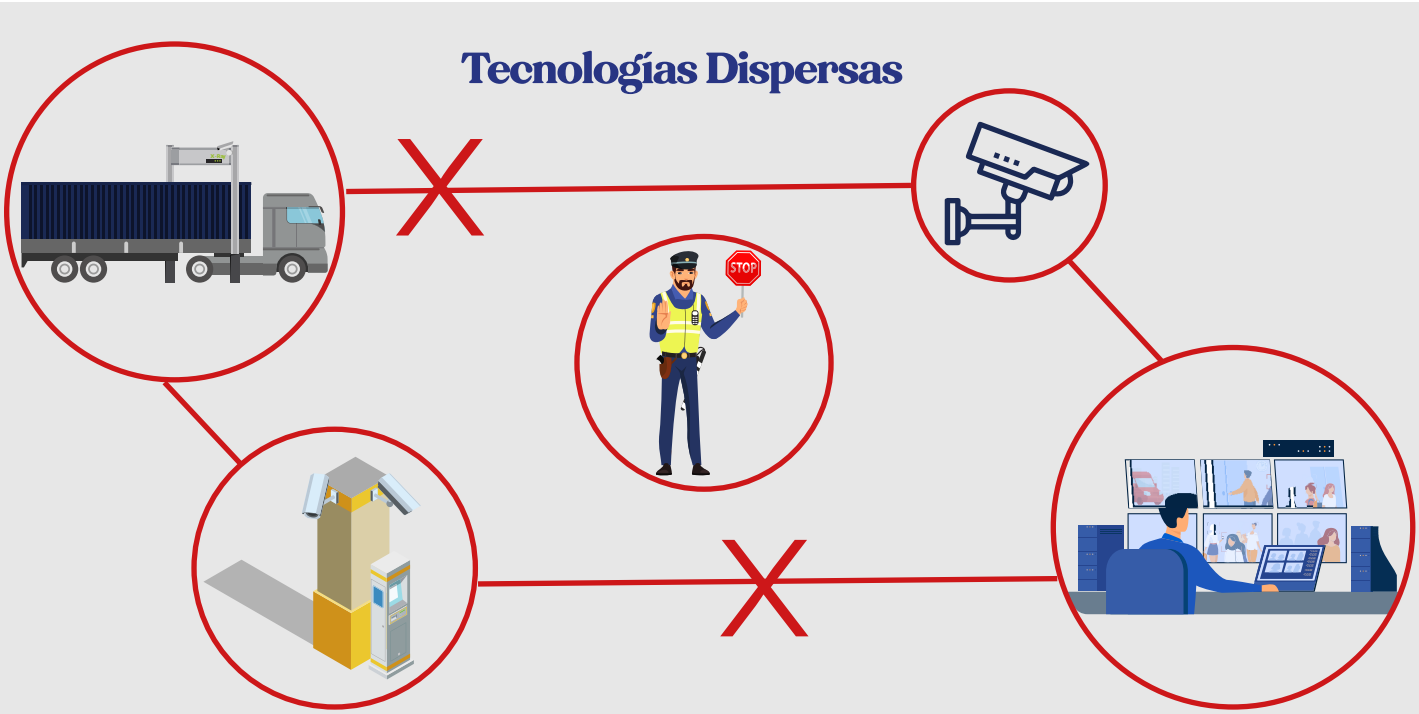
La protección portuaria efectiva trasciende los límites de la instalación. El intercambio oportuno de información entre la instalación portuaria y las instituciones con competencia en seguridad —Aduana, Guardia Costera, Policía Nacional Civil, organismos de inteligencia— multiplica la efectividad de 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.

ANEXOS

Definiciones Técnicas

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

Uso de Tecnologías Dispersas Vrs. Ecosistemas de Protección



ANDES
MONROVIA
IMO NO 9265366

Autoridad Designada
del Sistema Portuario Nacional

Autoridad Designada
del Sistema Portuario Nacional