Aperia

ICM
Potenciado por Tapestrii

SERIE PUERTOS BAJO PRESIÓN • Mayo de 2026

La Vulnerabilidad *Desde Adentro*

Las organizaciones criminales no vulneran los puertos de contenedores. Reclutan dentro de ellos.

7–20%

Valor de la carga pagado a estibadores corruptos por cada embarque facilitado (Europol, 2022)

~290 TM

Cocaína incautada en Ecuador en 2024, 30% por encima de 2023 (JIFE de la ONU, 2025)

4+

Los sistemas desconectados contienen las señales; nadie las ve en conjunto

TRES FALLAS. TODAS INVISIBLES.

VERIFICACIÓN ÚNICA

Los trabajadores aprobados al momento de la contratación no generan alerta cuando son reclutados años después

SEÑALES AISLADAS

Los registros de acceso, las consultas de manifiestos y los incidentes residen en sistemas separados

SOLO RETROSPECTIVO

Los patrones se vuelven visibles solo después de que la incautación los hace evidentes

tapestriisupport@aperia.com
www.aperia.com/platforms/tapestrii-icm

Considere un escenario armado a partir de patrones documentados en distintas terminales de América Latina (LATAM). Un estibador marca su entrada al patio de contenedores en un cambio de turno. Las credenciales son válidas. La ventana de acceso coincide con el rol asignado al trabajador. El relevo de turno está lo suficientemente ocupado para que el momento parezca rutinario. Dos meses después, la aduana de Róterdam intercepta un contenedor proveniente de esa terminal con varios cientos de kilogramos de cocaína ocultos en un cargamento refrigerado legítimo. La investigación retrospectiva revisa registros de acceso, consultas al manifiesto y reportes de incidentes. El patrón estaba ahí. Ningún sistema lo había armado.

Sin brecha. Sin intrusión. Una persona de confianza, ya adentro, se había convertido en el mecanismo. Esta es la amenaza que no parece una amenaza, porque operativamente, en tiempo real, se ve exactamente como trabajo normal. El resto de este documento examina por qué esa firma es tan difícil de detectar, y qué se requeriría para verla antes de que la incautación la haga visible.

La Arquitectura Del Acceso

Mover cocaína a escala no es un problema de intrusión. Es un problema de acceso.

El transporte marítimo en contenedores moviliza más de 720 millones de contenedores en el mundo cada año, lo que representa aproximadamente el 90 por ciento de la carga global.[1] Los volúmenes de cocaína que hoy salen de los puertos de LATAM (cientos de toneladas métricas anuales entre Ecuador, Colombia, Brasil y el Cono Sur) no se mueven a través de ese sistema por improvisación. Cada envío requiere códigos de contenedor, posiciones de bahía, ruteo de inspección, registros de precintos y tiempos de movimiento. Nada de esa información está disponible públicamente. Toda ella reside en las personas que trabajan en la terminal.

Las redes criminales se han organizado en torno a esta realidad estructural. El acceso desde adentro no es un recurso secundario cuando falla el contrabando externo. Es el mecanismo principal. En su análisis conjunto de abril de 2023 con el Comité Directivo de Seguridad de los puertos de Amberes, Hamburgo/Bremerhaven y Róterdam, Europol designó la corrupción del personal portuario (estibadores, empleados de logística y seguridad, funcionarios de aduana y de fuerzas del orden) como el “facilitador clave” de la infiltración criminal en los tres mayores puertos de Europa.[2] Las mismas dinámicas aplican hoy, con evidencia creciente, a los puertos de salida en LATAM.

La economía del reclutamiento ha escalado a la par. En octubre de 2022, una operación de la Guardia di Finanza italiana, con apoyo de Europol y Eurojust, desmanteló una red vinculada a la 'Ndrangheta que movía cocaína por el puerto de Gioia Tauro. La investigación documentó a coordinadores de campo pagando a estibadores corruptos comisiones del 7 al 20 por ciento del valor de la carga por envío facilitado, además de un funcionario de aduana corrupto que alteró el resultado de un escaneo de rayos X a cambio del 3 por ciento del valor de la carga. Los envíos incautados sumaron más de cuatro toneladas métricas de cocaína con un valor estimado en la calle superior a 800 millones de euros.[3] A esas tarifas, la parte que recibe un trabajador por un solo envío facilitado excede varios años de salario legítimo. Esto no es un pago oportunista. Es una estructura salarial paralela que compite con la oficial.

Lo que ha surgido en este panorama son los "especialistas", organizaciones facilitadoras que ofrecen un servicio llave en mano a las organizaciones de narcotráfico (DTOs, por sus siglas en inglés), tendiendo el puente entre las redes criminales y el personal portuario cuyo acceso necesitan. Sin ellas, mover volúmenes a través del transporte marítimo sería una proposición mucho más difícil.

Cómo Funciona El Reclutamiento

Tres vectores. Cada uno se manifiesta de forma distinta. Cada uno se explota de forma distinta. Los procesos estándar de Recursos Humanos no detectan ninguno.

Presión Financiera. Los estibadores ganan salarios modestos en proximidad directa con logística criminal de alto valor. La investigación de la 'Ndrangheta antes mencionada documentó tasas de comisión del 7 al 20 por ciento del valor de la carga por envío facilitado.[3] La guía sectorial de Skuld sobre contrabando de narcóticos en América Latina describe la misma dinámica de reclutamiento en Colombia, Ecuador, Perú, México, Brasil y Venezuela: los traficantes "requieren acceso a las áreas portuarias, por lo general a través del reclutamiento de conductores, empresas de transporte, estibadores y trabajadores de patio de contenedores corruptos" para cargar la droga en los contenedores.[4]

Vínculos Sociales Y Comunitarios. El empleo portuario en muchas terminales de LATAM concentra a trabajadores provenientes de los mismos barrios, las mismas familias y los mismos corredores migratorios. Las organizaciones criminales con raíces locales no se

acercan a desconocidos. La conversación inicial llega a través de un conocido o de un miembro de la familia extendida del trabajador que ya cruzó la línea. Para cuando se articula la solicitud de reclutamiento, ya existe una relación de obligación. Este es el vector que vuelve invisible al reclutamiento interno frente a los procesos estándar de Recursos Humanos.

Coacción. En entornos donde las organizaciones criminales ejercen un control efectivo sobre comunidades aledañas al puerto (documentado en Guayaquil, en zonas alrededor de Santos y en corredores específicos de Colombia y México),[5] negarse no es una opción segura. Los trabajadores cumplen no por incentivo, sino por la ausencia de alternativa. La violencia contra trabajadores que se resisten está documentada. Un solo caso, comunicado a través de las mismas redes familiares y vecinales antes descritas, es suficiente para establecer la regla.

Un escenario común en los puertos de LATAM hoy: personal clave recibe mensajes de WhatsApp con amenazas físicas específicas contra ellos y sus familias, a menudo con fotos o videos de sus hogares o seres queridos, acompañadas de una oferta monetaria para mirar hacia otro lado o proporcionar información. El mensaje mismo es el mecanismo de coacción.

Qué Entregan En Realidad Los Infiltrados

Distintos roles resuelven distintos cuellos de botella. Cada nivel representa un desafío de detección diferente.

La participación desde adentro no es una categoría aislada; corresponde al rol operativo del trabajador reclutado. El valor que se le entrega a la red criminal varía marcadamente según el nivel de acceso.

Manifiesto y posicionamiento del contenedor. Códigos de contenedor, asignaciones de bahía y tiempos de movimiento. La técnica de "fraude de código PIN" detectada por primera vez en Róterdam en 2018, en la que las redes criminales se apropian indebidamente del código único de referencia del contenedor necesario para retirar la carga, ilustra cómo un solo dato proporcionado desde adentro puede comprometer un envío entero.[2] Sin esa información, ningún otro nivel de acceso importa, porque la red criminal no sabe sobre qué contenedor actuar. Esta es la capa fundacional.

Ruteo de inspección. Qué contenedores son marcados para escaneo, cuándo y por quién. Esa información reside en supervisores de aduana y personal de seguridad portuaria. El acceso desde adentro a este nivel convierte un problema probabilístico (¿será escaneado mi contenedor?) en uno determinístico (sé que no lo será).

Acceso físico al patio. La operación de "rip-on/rip-off": ubicar el contenedor, romper el precinto, cargar o descargar el producto, reemplazar el precinto con una réplica de alta fidelidad. Esto requiere mano de obra portuaria o supervisores de patio con acceso físico legítimo durante la ventana relevante. El acto en sí toma minutos; el acceso necesario para ejecutarlo sin ser observado requiere coordinación entre varios roles.

Acceso a registros digitales. El nivel más valioso y menos discutido: trabajadores que pueden modificar registros de acceso, entradas en el manifiesto, registros de movimiento de contenedores o resultados de inspección con posterioridad. A medida que las operaciones portuarias se digitalizan, este nivel gana valor. Un registro digital limpio es más duradero que una operación física limpia, porque sobrevive a la investigación retrospectiva.

Estos niveles no son simplemente cuatro trabajos distintos. Son cuatro superficies de acceso distintas, cada una gobernada por un sistema de registro diferente, cada una bajo la responsabilidad operativa de un equipo diferente. La red criminal los trata como una sola capacidad coordinada. La terminal los trata como cuatro dominios operativos sin relación entre sí. Esa asimetría es la apertura.

Por Qué Los Controles Estándar No Lo Detectan

La seguridad portuaria fue diseñada para actores hostiles que intentan entrar. La amenaza interna invierte cada una de las suposiciones de ese modelo.

El argumento estructural es directo. Verificaciones de antecedentes, controles perimetrales, asignación de escáneres, accesos credencializados: cada capa de la arquitectura de seguridad portuaria asume un actor que no pertenece, intentando mover material que no es suyo. La amenaza interna invierte cada una de esas suposiciones. El actor pertenece allí. Las credenciales son válidas. El movimiento está autorizado. El material que se mueve es, sobre el papel, la carga legítima de alguien más. La arquitectura, por diseño, no registra lo que está ocurriendo, porque nada en ello se parece a un ataque.

Esta inversión tiene cuatro consecuencias operativas:

El modelo de tamizaje es de una sola vez, la amenaza es continua. Las verificaciones de antecedentes se hacen una vez, en la contratación, y capturan el historial hasta ese

momento. Un trabajador contratado limpio en 2019 y reclutado en 2022 no genera ninguna alerta, porque no existe mecanismo que vuelva a hacer la pregunta tras el onboarding. La Estrategia de Puertos de la UE de la Comisión Europea de marzo de 2026 propone explícitamente un marco a nivel de la UE para verificaciones continuas de antecedentes del personal portuario, con implementación prevista para 2027, precisamente porque dicho marco no existe en la actualidad.[6] Las verificaciones también suelen limitarse a registros de gobierno locales, en lugar de cruzarse con bases de datos internacionales o con señales sociales que revelarían asociaciones criminales, dificultad financiera o vínculos comunitarios con redes conocidas.

La unidad de análisis es el individuo, la unidad de compromiso es el rol. Los controles existentes están diseñados para preguntar "¿*es confiable esta persona*?". La pregunta operativamente relevante es otra: "¿es esta combinación de accesos, esta semana, consistente con la forma en que este rol opera habitualmente?". Un trabajador específico puede no llamar la atención. El rol ejecutado de forma poco llamativa es el problema completo, porque el rol es lo que la red criminal realmente alquiló.

Cada evento está autorizado; solo la secuencia es anómala. Acceso al patio fuera de horario el martes, una consulta inusual al manifiesto el miércoles, una retención de inspección liberada sin escaneo el jueves. Cada evento, en aislamiento, es trabajo legítimo ejecutado por una persona autorizada. No hay anomalía individual que escalar. La señal es la secuencia, y una arquitectura de seguridad organizada en torno a la autorización por evento no tiene un concepto nativo de la secuencia como unidad de revisión.

La detección es retrospectiva por diseño. Para cuando una investigación de incautación en Róterdam o Amberes reconstruye la cadena hasta el puerto de salida, la operación típicamente ya se ejecutó múltiples veces. Las señales estuvieron presentes en los datos todo el tiempo. "Retrospectiva" es la palabra clave: describe una postura de seguridad organizada en torno a explicar lo que pasó, no a interrumpir lo que está pasando. Esa es una postura defendible frente a una amenaza externa donde las intrusiones son eventos discretos. Colapsa frente a una amenaza interna donde la operación es continua y el siguiente envío ya está en marcha.

Un ejemplo aclara qué se está dejando pasar y lo prosaicamente que aparece cuando alguien efectivamente lo busca. Un analista de seguridad de un puerto de LATAM comenzó a revisar los registros de asistencia y notó que la llegada de un buque específico se correlacionaba con una reducción cercana al 30 por ciento del personal en turno. No una vez. Cada

vez que ese buque atracaba. Al entrevistar a los empleados, el analista supo que entre el personal portuario era ampliamente conocido cuándo los actores ilícitos planeaban contaminar contenedores, y esos intentos coincidían con un buque específico de ruta mediterránea. Los trabajadores honestos optaban por incapacidades o días personales antes que convertirse en testigos de la actividad ilegal y en posibles objetivos de las DTOs. La señal estaba en los datos de nómina. Ningún protocolo existente le hacía esa pregunta a los datos de nómina.

El Problema De Escala

Detectar a un infiltrado es difícil. Detectar una red de infiltrados es un problema completamente distinto.

El reclutamiento interno a veces se discute como una historia de un solo mal actor. Los datos no respaldan ese encuadre. Los volúmenes de cocaína que hoy se mueven por los puertos de LATAM requieren logística coordinada en múltiples movimientos de contenedores por envío, y cada movimiento requiere su propia facilitación interna. Mientras las incautaciones de Ecuador en 2024 alcanzaron niveles récord, la aduana belga en el puerto de Amberes registró una caída pronunciada, de 121 toneladas métricas incautadas en 2023 a 44 toneladas métricas en 2024.[7] La presión de las autoridades en un nodo redirige el volumen en lugar de reducirlo. Mover esos volúmenes no es trabajo de un solo trabajador corrompido; es trabajo de una red incrustada.

Las investigaciones de Europol en Amberes, Hamburgo/Bremerhaven y Róterdam lo han documentado directamente: la corrupción interna opera como redes internas organizadas, distribuidas entre empresas de logística, servicios aduaneros y operaciones de seguridad de manera simultánea.[2] Trabajadores de distintos departamentos, en distintos turnos, con distintos niveles de acceso, coordinan para facilitar un solo envío. La estructura es deliberada. Está diseñada para derrotar exactamente el tipo de monitoreo de un solo actor que la mayoría de las operaciones de seguridad portuaria tienen implementado.

Esto cambia el problema de detección de forma fundamental. Identificar a un solo trabajador corrompido mediante monitoreo conductual es difícil pero abordable; con el tiempo se acumulan suficientes anomalías como para llamar la atención. Identificar el patrón que conecta a múltiples trabajadores corrompidos en distintos roles, departamentos y turnos es una capacidad enteramente distinta. Requiere inteligencia a nivel de entidad: la habilidad de preguntar no solo *"¿se comportó este trabajador de forma anómala?",* sino

"*¿estos trabajadores, individualmente poco llamativos, comparten un patrón inusual de coocurrencia con los mismos contenedores marcados, los mismos proveedores o los mismos incidentes?*". Esa pregunta no puede ser respondida por ningún sistema que la mayoría de las terminales de LATAM opera hoy, porque la pregunta misma no está en el vocabulario operativo de esos sistemas.

La amenaza interna no es un problema de personal. Es un problema de inteligencia conductual a nivel de la red, no del trabajador. Esa es una categoría de pregunta que la mayoría de las operaciones de seguridad portuaria aún no se está haciendo.

Qué Requiere Realmente La Detección

Lo difícil no es recolectar más datos. Lo difícil es hacerle a los datos una pregunta que nunca antes se les ha hecho.

Es tentador describir la brecha como un problema de integración de datos y detenerse ahí. Ese encuadre es incompleto y, en la práctica, engañoso. A la mayoría de las terminales de LATAM no les faltan datos. Les falta la pregunta operativa que haría que sus datos existentes respondieran algo útil. La actividad interna es, por construcción, indistinguible del trabajo legítimo a nivel de cualquier evento aislado. Solo se vuelve visible cuando los datos son interrogados con una pregunta diseñada para el modelo de amenaza real: no "¿qué ocurrió?", sino "¿qué combinaciones de personas, accesos y carga han coocurrido de formas que el ritmo operativo legítimo de esta terminal no explica?".

Se requieren cuatro desplazamientos, en este orden. El orden importa. Invertirlo es lo que produce los tableros que nadie usa.

Del evento a la entidad. La mayoría de los sistemas portuarios se organizan en torno a eventos: una marcación, una consulta, un cambio en el manifiesto, un reporte de incidente. Las operaciones internas se organizan en torno a entidades: este trabajador, este proveedor, este buque, este contenedor, este corredor. Un sistema organizado por eventos puede describir un turno; solo un sistema organizado por entidades puede describir una relación. La primera capacidad que hay que construir no es un tablero. Es un modelo de entidades en el que cada evento, a través de cada sistema fuente, se vincule limpiamente a las personas y cosas a las que realmente concierne.

De la anomalía a la coocurrencia. Ningún evento aislado en una operación interna es anómalo, por lo cual la detección por evento produce ruido y pierde el patrón. La señal relevante es la coocurrencia: los mismos tres trabajadores, en el mismo turno, alrededor del mismo proveedor, en proximidad a los mismos contenedores marcados, a lo largo de tres envíos facilitados distintos. Ninguna anomalía individual. La coocurrencia es la anomalía.

Del incidente al expediente. Un solo incidente casi nunca prueba participación interna. Un trabajador asociado con tres contenedores marcados a lo largo de dieciocho meses, sí. Pero "asociado con" no es un campo en ningún sistema operativo; es el producto de una documentación que se acumula contra una entidad a lo largo del tiempo. Sin una capa de expediente, cada investigación parte de cero. La entidad no tiene memoria. Las redes internas dependen de eso.

De datos internos a señales externas. Las presiones de reclutamiento (dificultad financiera, asociaciones criminales, vínculos comunitarios) aparecen en fuentes externas, no en los sistemas de la terminal. Una arquitectura de detección limitada a los datos que la terminal misma genera es, por construcción, ciega a los vectores de reclutamiento descritos en la Sección 2. La terminal ve el acceso. El reclutamiento vive en otro lugar.

Una nota final sobre lo que esto no es. No es una recomendación de comprar más cámaras, escáneres o lectores. La mayoría de los puertos de LATAM ya los tiene. Tampoco es un llamado a consolidar todos los sistemas en uno. Lo que se requiere es una capa delgada de entidad y coocurrencia que lea a través de los sistemas existentes sin reemplazarlos.

Fuentes

1. UN News, UN-Backed Programme Logs Record High Cocaine Seizures at Seaports in Latin America and the Caribbean (2018), citando el Programa de Control de Contenedores de la UNODC: más de 720 millones de contenedores se mueven por vía marítima anualmente, transportando aproximadamente el 90 por ciento de la carga global.

2. Europol y el Comité Directivo de Seguridad de los Puertos de Amberes, Hamburgo/Bremerhaven y Róterdam, Criminal Networks in EU Ports: Risks and Challenges for Law Enforcement: Focus on the Misappropriation of Container Reference Codes (La Haya: Europol, 30 de marzo de 2023). Designación de la corrupción del personal portuario como el "facilitador clave" de la infiltración criminal; técnica de apropiación indebida de códigos PIN detectada por primera vez en Róterdam en 2018.

3. Comunicado de prensa de Europol, Italian Operation Takes Down Corrupt Port Workers Facilitating 'Ndrangheta Drug Trafficking Activities: Customs Officer Features Among the Arrested (6 de octubre de 2022). Operación conjunta de la Guardia di Finanza italiana, Europol y Eurojust en Gioia Tauro: comisión del 7 al 20 por ciento a estibadores corruptos; 3 por ciento a un funcionario de aduana corrupto por alterar un escaneo de rayos X; más de 4 toneladas métricas de cocaína incautadas; valor en la calle estimado superior a 800 millones de euros.

4. Skuld P&I, Colombia: Drug Smuggling: Update (2022). Reclutamiento de conductores, empresas de transporte, estibadores y trabajadores de patio de contenedores corruptos como el mecanismo operativo detrás de la contaminación de contenedores en los puertos de salida latinoamericanos.

5. International Crisis Group, Curbing Violence in Latin America's Drug Trafficking Hotspots, Informe N.º 108 (marzo de 2025). Documentación del control del crimen organizado sobre comunidades aledañas al puerto en Guayaquil, Santos y corredores en Colombia y México.

6. Comisión Europea, EU Ports Strategy: Securing Competitive, Resilient and Sustainable European Ports (marzo de 2026). Propone un marco de la UE para verificaciones de antecedentes del personal portuario (previsto para 2027) y marcos para evaluaciones de puertos de terceros países, sobre la base de la European Ports Alliance.

7. InSight Crime, InSight Crime's 2024 Cocaine Seizure Round-Up (abril de 2025). La aduana belga incautó 44 toneladas métricas de cocaína en Amberes en 2024, una caída pronunciada frente a las 121 toneladas métricas de 2023; el análisis atribuye el cambio, en parte, al desplazamiento impulsado por la presión de las autoridades.

Sobre La Serie Puertos Bajo Presión

Este es el segundo documento de una serie de cuatro partes que examina los desafíos en evolución que enfrentan los puertos de contenedores latinoamericanos. El Documento Uno analizó cómo las redes criminales seleccionan puertos como nodos de salida. Este documento, el Documento Dos, examina la amenaza interna que vuelve operativamente viables a esos puertos. El Documento Tres abordará la fragmentación de los sistemas de seguridad portuaria y lo que esa fragmentación cuesta. El Documento Cuatro definirá la arquitectura integrada de inteligencia que se requiere para cerrar la brecha. Para recibir los documentos restantes de la serie o para discutir cómo estos temas están afectando a su puerto o terminal, contáctenos en tapestriisupport@aperia.com.

Sobre Aperia

Aperia ofrece ICM by Tapestrii, una plataforma inteligente de gestión de casos que ayuda a operadores de terminales y autoridades portuarias a conectar incidentes, entidades y datos operativos fragmentados para detectar riesgos emergentes con mayor antelación y fortalecer la toma de decisiones en entornos complejos y de alto riesgo. Damos la bienvenida al diálogo con operadores portuarios, gerentes de terminales y líderes de seguridad comprometidos con anticiparse a estas dinámicas. Conozca más en www.aperia.com.

James Kuykendall es ex Director Regional Asistente de la DEA con amplia experiencia operativa en América Latina y consultor en ejercicio en seguridad marítima.

Viviana Lewis es Gerente de Producto en Aperia, lidera producto y éxito global de clientes para ICM by Tapestrii.