CONECTARSE

Lun, 14 Diciembre 2015 | 11:50

ENCUENTRO T21 | ECONOMÍA | T21 PANAMÁ | CAMBIOS APIS | LEY FERROVIARIA | PNI |

TERCER INFORME DE GOBIERNO

Las 6 recomendaciones de la CIP sobre ciberseguridad portuaria

Mié, 09/09/2015 - 12:10pm Por: Luis Alberto Zanela 1150 lecturas Imprimir E-Mail

Archivado en: | Marítimo | cibercrimen | Comisión Interamericana de Puertos (CIP) | Jorge Durán

Jorge Durán, Jefe de la Secretaría de la Comisión Interamericana de Puertos (CIP)

Twitteár
G+1 1
Share 9

MÉRIDA, YUC.- **El número de aparatos conectados a Internet superó a la población mundial en 2008 y continúa creciendo.** En 2013 había 13 mil millones de conexiones máquina a máquina y se estima que para 2020 habrá más de 50 mil millones, según estimaciones del Government Executive de Estados Unidos.

Ante ello, el transporte marítimo y los puertos no son excepción, por lo cual cobra importancia la protección a la ciberseguridad de procesos automatizados o electrónicos, ya que se han experimentado ataques en 88 países e incluso a páginas de Internet reconocidas en la industria, como Marine Traffic, de acuerdo con Jorge Durán, Jefe de la Secretaría de la Comisión Interamericana de Puertos (CIP), de la Organización de los Estados Americanos (OEA).

En ese sentido, **la CIP recomienda un Ciclo de Retroalimentación que consiste en seis recomendaciones para evitar ciber ataques en los procesos portuarios**:

1.- Evalúa: Evaluar dónde está el estado de riesgo mediante pruebas e implementar las mejores prácticas internacionales.

2.- Mitiga: Establecer un presupuesto, las mejores prácticas internacionales e implementar soluciones.

3.- Capacita: Instrumentar un programa de capacitación en ciberseguridad para ejecutivos y el mayor número de empleados posible.

4.- Transfiere: Explorar un seguro de ciberseguridad, así como se aseguran otros activos del puerto como la infraestructura.

5.- Toma acción: Contratar a terceros como expertos, probar esfuerzos y medir riesgos. Una especie de auditoría de un tercero que evalúe los servicios tecnológicos en el recinto.

6.- Institucionaliza: Hacer del programa del manejo de riesgos de ciberseguridad una práctica permanente en el puerto, destinando herramientas y presupuestos.

La creciente dependencia en sistemas automatizados hace a las cadenas globales y locales de suministro vulnerables a los ataques criminales y terroristas o al uso de los puertos para perpetrarlos, lo cual hace patente y urgente llevar a cabo las acciones anteriores en los recintos, explicó Jorge Durán durante su participación en el Foro internacional sobre seguridad y protección marítima-portuaria, organizado por la Red PBIP Internacional en esta ciudad.

Twitter: @BetoZanela

RECOMENDACIONES PARA PROSEGUIR LA LECTURA:

Equilibrio competitividad-protección, reto de seguridad portuaria

Reducirán emisión de gases de buques en puertos mexicanos