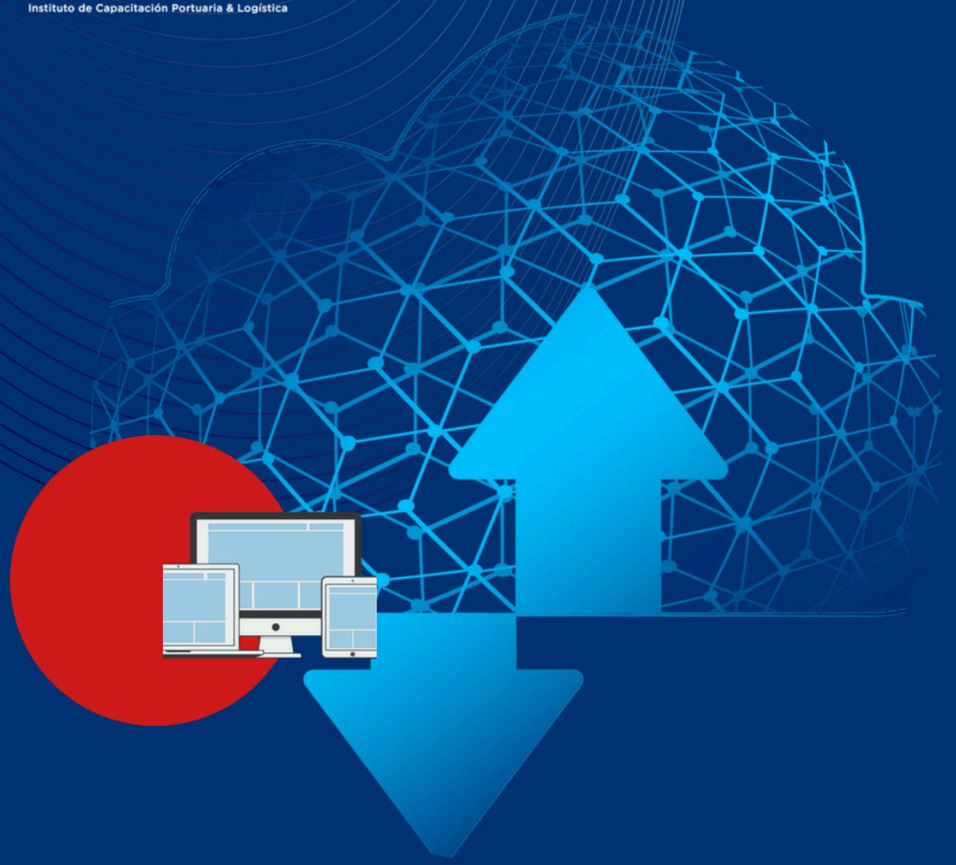
INPLOG

Instituto de Capacitación Portuaria & Logística

Programa:

MITIGANDO RIESGOS DE CIBERSEGURIDAD Y SEGURIDAD PERIMETRAL EN LA CADENA DE SUMINISTRO Y LOGÍSTICA.

INPLOG
Instituto de Capacitación Portuaria & Logística



DESCRIPCIÓN GENERAL:

Este programa está diseñado para capacitar a profesionales clavesenlaindustria logística y marítima en general, sobre las amenazas y vulnerabilidades cibernéticas específicas que enfrentan en sus operaciones diarias. A lo largo del programa, los participantes adquirirán una comprensión profunda de las estrategias y mejores prácticas para identificar, evaluar y mitigar los riesgos cibernéticos en toda la cadena de suministro marítima. Desde la seguridad de los sistemas de información hasta la protección de datos críticos y la prevención de ciberataques, proporcionaremos las herramientas y el conocimiento necesario para salvaguardar los activos digitales y garantizar la continuidad de las operaciones en un entorno cada vez más digitalizado y conectado.

INPLOG
Instituto de Capacitación Portuaria & Logística

OBJETIVOS ESPECÍFICOS

- Identificar y comprender las principales amenazas cibernéticas que enfrenta la cadena de suministro marítima, incluidos los riesgos asociados con la interconexión de sistemas digitales y la dependencia de tecnologías de información y comunicación.

- Evaluar la infraestructura y los sistemas de información utilizados en la cadena de suministro para identificar posibles puntos de vulnerabilidad y debilidades en la seguridad cibernética.

- Diseñar e implementar estrategias efectivas de mitigación de riesgos cibernéticos que aborden los desafíos específicos de seguridad en la cadena de suministro, incluyendo la protección de datos críticos, la prevención de intrusiones y la respuesta rápida a incidentes de seguridad.

- Capacitar al personal clave, incluidos gerentes de TI, profesionales de logística y líderes empresariales, en el desarrollo de competencias técnicas y prácticas para proteger los activos digitales y garantizar la continuidad operativa frente a amenazas cibernéticas.

- Fomentar una cultura de seguridad cibernética proactiva y colaborativa dentro de las organizaciones relacionadas con la cadena de suministro marítima, promoviendo la conciencia y el compromiso de todos los miembros del equipo en la protección de la infraestructura digital y los datos confidenciales.

DIRIGIDO A :

•Profesionales delogística: Encargados de la planificación y ejecución de las operaciones logísticas en la cadena de suministro.

·Directivos y ejecutivos de empresas relacionadas con la industria: Líderes empresariales con interés en comprender y mitigar los riesgos cibernéticos en la cadena de suministro.

·Gerentes de TI: Profesionales responsables de la administración y coordinación de los recursos tecnológicos de la organización.

• Directores de seguridad de la información: Profesionales que supervisan y ejecutan las estrategias de seguridad de la información.

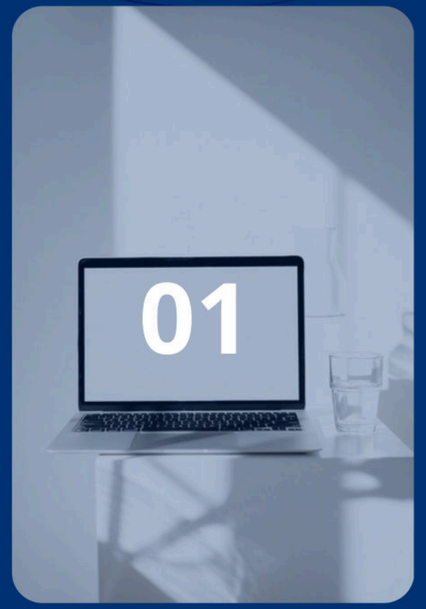
• Gerentes de cadena de suministro: Responsables de la gestión y coordinación de la cadena de suministro en empresas del sector logístico.

• Profesionales de ciberseguridad: Expertos en seguridad informática con conocimientos específicos sobre la protección de activos digitales en entornos marítimos.

INPLOG
Instituto de Capacitación Portuaria & Logística

CONTENIDO DEL PROGRAMA

MÓDULO



1. Panorama actual de la ciberseguridad en la industria:

-Retos

-Ataques recientes.

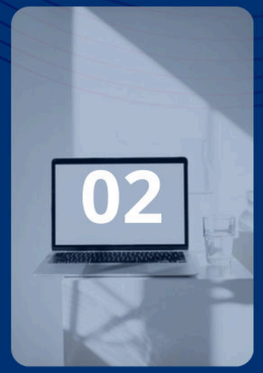
2. Fundamentos de ciberseguridad:
¿Qué es la ciberseguridad, a quién afecta, cómo y por qué?
- Enumerar riesgos asociados para los negocios.
¿Qué son las vulnerabilidades y que se entiende por amenazas?
¿Cuáles son las necesidades de seguridad de los negocios en la industria de logística?
- Beneficios de estar protegido

3. Conoce a tu enemigo:
- Principales amenazas
- Actores
-Amenazas internas
-Formación a los empleados
-Caso de estudio - Modelo de amenazas.

4. Conócete a tu empresa:
- Importancia de la información.
¿Qué son los activos de información?
-¿Qué es el riesgo?
-Tipo de riesgo y su gestión.
- Caso de estudio – Matriz de riesgos tecnológicos.

CONTENIDO DEL PROGRAMA

MÓDULO



•1.**Ingeniería social:**

- Definición de ingeniería social.

- Valor de nuestra información en internet.

- Tipos de ataque de ingeniería social.

- Concientización y mecanismos de defensa.

2.Seguridad en redes sociales y IOT:

-Riesgos asociados.

-Controles de seguridad.

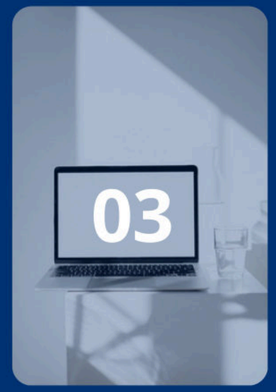
3. Seguridad en dispositivos móviles y redes wifi.

¿Por qué proteger los dispositivos móviles?.

¿Cómo disminuir el riesgo?

- Seguridad en redes wifi

MÓDULO



1.Marcos de seguridad, estándares y manejo de riesgos:

-Marco y estándares de ciberseguridad.

-Evaluación y gestión de riesgos.

- Caso de estudio – Controles CIS.

2.Planificación de respuesta a incidentes:

- Gobernar

-Identificar - Proteger - Detectar - Responder - Recuperar

3.Caso de estudio - Gestión de respuesta ante incidentes.

FACILITADORES

Este programa se ha realizado en colaboración conlaorganizaciónCyberWarrior.com, con sede en Boston, y serádictadopor facilitadoresinternacionales.

Magister Sheila Pérez

Profesional experimentada en Tecnologías de la Información con más de dos décadas de experiencia, ha desempeñado diversos roles que le han proporcionado una comprensión integral de diversas especialidades. Su historial incluye la propuesta, diseño, desarrollo e implementación de proyectos de forma individual, así como el liderazgo de equipos en implementaciones impulsadas por proveedores, mientras gestiona recursos y garantiza la entrega oportuna. En el ámbito de la estrategia de ciberseguridad, dirige y coordina esfuerzos para salvaguardar procesos empresariales e información para una importante terminal portuaria en Panamá. Su experiencia se extiende al manejo de proyectos, soluciones innovadoras y migraciones de plataformas. Más allá de sus esfuerzos profesionales, contribuye activamente a la comunidad. Como COO de la Fundación Comunidad DOJO y el Capítulo de Mujeres de Seguridad de Panamá, lidera campañas educativas sobre concienciación en ciberseguridad para profesionales y el público en general. Además, se desempeña como coanfitrión en el podcast "Impulso Cyber", dirigido a profesionales de la ciberseguridad y aquellos que buscan mantenerse informados en el campo.

Magister Eduardo Snape

Cuenta con más de 3 décadas de experiencia profesional, actualmente es el director ejecutivo de la Fundación Comunidad DOJO, una organización dedicada a la formación en ciberseguridad para todos, ocupa el cargo de director de tecnología para una firma de abogados panameña con alcance internacional. Además, se destaca como docente universitario, Instructor en temas de ciberseguridad, consultor en tema de transformación digital y ciberseguridad. Fue seleccionado por la embajada de Estados unidos en Panamá para participar en el International Visitor Leadership Program 2021, una iniciativa del Departamento de Estado de los Estados Unidos.