Maritime Cyber Security Meeting Kit – Spanish

QUÉ ESTÁ EN RIESGO

La ciberseguridad marítima se refiere a la protección de los sistemas de tecnología de la información, las redes y los datos de la industria marítima frente a las ciberamenazas. Se trata de aplicar medidas y prácticas para proteger los buques, las infraestructuras en tierra, las redes de comunicación, los sistemas portuarios y la cadena de suministro internacional frente a posibles ciberataques.

CUÁL ES EL PELIGRO

PRINCIPALES PELIGROS ASOCIADOS A LA CIBERSEGURIDAD MARÍTIMA

- Los ciberataques pueden interrumpir las operaciones marítimas, si los sistemas críticos de un buque se ven comprometidos interrumpiendo la navegación, la manipulación de la carga o las comunicaciones.
- Las ciberamenazas pueden afectar al funcionamiento de sistemas críticos para la seguridad, como la extinción de incendios, la respuesta de emergencia y los equipos de salvamento, poniendo vidas en peligro.
- Los piratas informáticos comprometen los sistemas que controlan la gestión del agua de lastre o las operaciones de transferencia de combustible, lo que provoca incidentes de contaminación, como el vertido accidental de sustancias nocivas en el agua.
- Los ciberatacantes pueden explotar las vulnerabilidades de los sistemas portuarios o los procesos de la cadena de suministro para obtener acceso no autorizado a la información sobre la carga o manipular los documentos de embarque, lo que puede provocar pérdidas, robos o poner en peligro la integridad de la cadena de suministro.

- Un ciberataque exitoso puede resultar en el robo o acceso no autorizado a la propiedad intelectual, comprometiendo la competitividad, los secretos comerciales y los derechos de propiedad intelectual.
- Los sistemas marítimos almacenan y transmiten información sensible, incluidos datos personales, registros financieros e información comercial confidencial. Una violación de los datos o de la privacidad puede dañar la reputación, acarrear sanciones reglamentarias y responsabilidades legales.
- Un ciberataque dirigido contra sistemas portuarios, proveedores logísticos o compañías navieras puede interrumpir el comercio mundial, retrasar los movimientos de carga y crear impactos económicos más allá del sector marítimo.
- Las amenazas a la ciberseguridad marítima pueden dedicarse al ciber espionaje, el sabotaje u otras actividades maliciosas para obtener ventajas geopolíticas o perturbar infraestructuras críticas.
- Una cobertura insuficiente de los seguros cibernéticos en el sector marítimo puede plantear problemas a la hora de recuperar las pérdidas financieras ocasionadas por incidentes cibernéticos.

COMO PROTEGERSE

A MEDIDAS EFICACES PARA ABORDAR LA CIBERSEGURIDAD MARÍTIMA

- Llevar a cabo una evaluación exhaustiva de las vulnerabilidades y riesgos potenciales de los sistemas, redes e infraestructuras marítimas. Identificar los activos críticos, evaluar su valor y determinar el impacto potencial de las ciberamenazas en las operaciones, la seguridad y la protección.
- Crear una estrategia de ciberseguridad que incluya políticas, procedimientos y directrices para mitigar los riesgos y protegerse contra las ciberamenazas.
- Desplegar una serie de medidas de seguridad técnicas y organizativas que incluyan cortafuegos, sistemas de detección de intrusos, cifrado, configuraciones seguras,

controles de acceso y actualizaciones periódicas de seguridad.

- Fomentar una cultura de concienciación sobre la ciberseguridad y promover un comportamiento responsable en relación con la protección de datos, la gestión de contraseñas y la prevención del phishing.
- Desarrollar un plan de respuesta a incidentes bien definido que describa los procedimientos de detección, contención, análisis, recuperación y comunicación de incidentes.
- Establecer foros o plataformas para compartir información, inteligencia sobre amenazas, mejores prácticas y lecciones aprendidas para adelantarse a la evolución de las ciberamenazas.
- Garantizar el cumplimiento de los marcos de ciberseguridad internacionales y regionales para satisfacer los requisitos mínimos de seguridad y mantener la confianza de las partes interesadas.
- Aplicar prácticas de gestión de proveedores que incluyan requisitos de seguridad, auditorías y obligaciones contractuales para minimizar los riesgos de la cadena de suministro.
- Realizar periódicamente evaluaciones de vulnerabilidad, pruebas de penetración y auditorías de seguridad para identificar puntos débiles y abordarlos con prontitud.
- Fomentar la notificación de actividades sospechosas, proporcionar canales para notificar incidentes y recompensar las prácticas proactivas de ciberseguridad.
- Aproveche los avances en tecnologías como la inteligencia artificial, el aprendizaje automático y el análisis del comportamiento para mejorar las capacidades de detección y respuesta ante amenazas.
- Revisar y actualizar periódicamente las medidas, políticas y procedimientos de seguridad para hacer frente a las nuevas amenazas y vulnerabilidades.

MEJORES PRÁCTICAS DE CIBERSEGURIDAD MARÍTIMA DEL TRABAJADOR

- Empiece por informarse sobre los fundamentos de la ciberseguridad marítima. Lea libros, artículos y

publicaciones del sector sobre el tema.

- Siga fuentes acreditadas, blogs del sector y medios de comunicación que cubran la ciberseguridad y la tecnología marítima para mantenerse al día de las nuevas amenazas y estrategias de mitigación.
- Considere la posibilidad de seguir programas de capacitación y certificación centrados en la ciberseguridad marítima.
- Asista a conferencias, seminarios y webinarios relacionados con la ciberseguridad marítima.
- Unirse a redes profesionales y comunidades en línea dedicadas a la ciberseguridad marítima.
- Establezca buenas prácticas personales de ciberseguridad marítima, como la gestión de contraseñas seguras, la actualización periódica del software, la precaución ante los correos electrónicos de phishing y la seguridad de sus dispositivos personales.
- Participe en actividades de autoaprendizaje, cursos en línea, seminarios web o talleres para profundizar sus conocimientos sobre las tecnologías emergentes y las ciberamenazas en evolución.
- Participe activamente en iniciativas de intercambio de información. Únase a foros, listas de correo o plataformas en línea donde los profesionales debatan sobre ciberseguridad marítima.
- Considere la posibilidad de encontrar un mentor que pueda orientarle y compartir su experiencia en ciberseguridad marítima.

CONCLUSIÓN

Al dar prioridad a la Ciber resiliencia y adoptar medidas de seguridad proactivas, el sector marítimo puede mejorar su capacidad de protección frente a las ciberamenazas y mantener unas operaciones seguras y eficientes.