

ATV Safety and Gear Stats and Facts

FACTS

Common Causes of ATV Accidents:

1. Inexperience with operating ATVs and lack of training can lead to accidents.
2. Riding an ATV at excessive speeds increases the risk of losing control, especially on uneven terrain.
3. Engaging in risky maneuvers, such as sharp turns, jumps, or wheelies, can lead to accidents.
4. Poorly maintained ATVs can experience mechanical failures that can lead to accidents.
5. Operating an ATV while under the influence of alcohol or drugs significantly impairs judgment.
6. Hazards in the environment, such as rough or uneven terrain, rocks, tree stumps, or other obstacles.
7. Ill-fitting helmets or gear that does not provide sufficient protection.
8. Carrying more passengers than the ATV is designed for can affect its stability and maneuverability.
9. Accidents can occur when ATVs collide with other vehicles, objects, or when encountering other riders on trails.
10. Weather conditions, such as rain, snow, mud, or ice, can affect the handling and traction of an ATV.
11. Rollover accidents are a big risk with ATVs traveling at high speeds or on uneven terrain.
12. Failing to wear helmets increases the risk of head injuries, like traumatic brain injuries.
13. Riding without goggles or a face shield can expose the rider to flying debris and insects.
14. Without proper protective clothing like gloves, long-sleeved shirts, and pants, riders are more vulnerable to cuts, scrapes, and lacerations in case of falls or contact with

rough surfaces.

STATS

- Every year nationwide approximately 135,000 individuals are injured in ATV-related accidents.
- The age group of 35 to 44 had the highest percentage of ATV operators involved in fatal crashes with a blood alcohol concentration (BAC) of 0.08% or higher, reports the (NHTSA) crash statistics.
- The Consumer Protection Safety Commission keeps track of all of the injury and death reports related to ATVs. For the latest reporting there were:93,800 ATV injuries treated in emergency rooms throughout the country. There is an average of 500-600 fatalities each year due to ATV accidents.
- There were 15,250 reported ATV deaths in the United States and millions of injuries. According to the CPSC, there have been 702 reported deaths.
- (CPCS) reported that in recent years an estimated 25,500 individuals were treated for ATV-related injuries in hospital emergency rooms; nearly 0,000 were hospitalized and over 400 deaths were recorded. Over 30 % of the injured persons were less than 6 years of age with 27 % of the fatalities to children under 6 years of age. The CPSC also indicated that 6.4 % of all ATV accidents occurred on the farm, resulting in more than 20 fatalities on American farms annually.
- In Canada, 33% of victims of fatal ATV accidents were not wearing a helmet.

ATV Safety and Gear Stats and

Facts – Spanish

HECHOS

Causas comunes de los accidentes de ATV:

1. La inexperiencia en el manejo de los ATV y la falta de capacitación pueden provocar accidentes.
2. Conducir un ATV a velocidades excesivas aumenta el riesgo de perder el control, especialmente en terrenos irregulares.
3. Realizar maniobras arriesgadas, como giros bruscos, saltos o caballitos, puede provocar accidentes.
4. Los ATV mal mantenidos pueden sufrir fallos mecánicos que pueden provocar accidentes.
5. Manejar un ATV bajo los efectos del alcohol o las drogas perjudica considerablemente la capacidad de juicio.
6. Peligros en el entorno, como terreno accidentado o irregular, rocas, tocones de árboles u otros obstáculos.
7. Cascos mal ajustados o equipos que no proporcionan suficiente protección.
8. Llevar más pasajeros de los previstos en el ATV puede afectar a su estabilidad y maniobrabilidad.
9. Los accidentes pueden ocurrir cuando los ATV chocan con otros vehículos, objetos o al encontrarse con otros conductores en los senderos.
10. Las condiciones meteorológicas, como lluvia, nieve, barro o hielo, pueden afectar a la maniobrabilidad y tracción de un quad.
11. Los accidentes por vuelco son un gran riesgo con los ATV que circulan a gran velocidad o por terrenos irregulares.
12. No llevar casco aumenta el riesgo de lesiones en la cabeza, como los traumatismos craneoencefálicos.
13. Conducir sin gafas o sin careta puede exponer al conductor a la proyección de escombros e insectos.
14. Sin la ropa de protección adecuada, como guantes, camisas de manga larga y pantalones, los motoristas son más vulnerables a cortes, rasguños y laceraciones en caso de caídas o

contacto con superficies rugosas.

ESTADÍSTICAS

- Cada año en todo el país aproximadamente 135.000 personas resultan heridas en accidentes relacionados con vehículos todo terreno.
 - El grupo de edad de 35 a 44 años tiene el porcentaje más alto de conductores de ATV implicados en accidentes mortales con una concentración de alcohol en sangre (BAC) de 0,08% o superior, según informan las estadísticas de accidentes de la NHTSA.
 - La Comisión de Seguridad y Protección de los Consumidores lleva un registro de todos los informes de lesiones y muertes relacionados con los ATV. Para el último informe hubo: 93.800 lesiones ATV tratados en salas de emergencia en todo el país. Hay una media de 500-600 muertes al año por accidentes de ATV.
 - Se han registrado 15.250 muertes por ATV en Estados Unidos y millones de heridos. Según la CPSC, se han registrado 702 muertes.
 - (CPCS) informó de que en los últimos años unas 25.500 personas fueron atendidas por lesiones relacionadas con ATV en las salas de urgencias de los hospitales; casi 0.000 fueron hospitalizadas y se registraron más de 400 muertes. Más del 30% de los heridos eran menores de 6 años y el 27% de los fallecidos eran niños menores de 6 años. La CPSC también indicó que el 6,4% de todos los accidentes con ATV se produjeron en la granja, lo que provocó más de 20 muertes anuales en las granjas estadounidenses.
 - En Canadá, el 33% de las víctimas de accidentes mortales con ATV no llevaban casco.
-

ATV Safety and Gear Fatality File

Farmer Dies Two Weeks After ATV Rollover

Frank hung in there “until the cows came home,” but in the end he couldn’t bargain with a blood clot.

The 66-year-old Wisconsin farmer died two weeks after his all-terrain vehicle (ATV) rolled on top of him during a fence-fixing project. The week he was going to be discharged from the hospital, he unexpectedly died when getting out of bed. The cause of death was respiratory failure due to a pulmonary embolism (blood clot).

The Investigation

According to the investigation, Frank had finished fixing a fence that was damaged by a windstorm. He was driving his ATV slowly down a hill when he tried to maneuver over a small tree growing out of a stump. Frank assumed the ATV’s tires would crush the tree, but they didn’t. Instead, the machine tipped over, causing him to fall down a 20-foot (six-meter) embankment. The ATV followed Frank down the hill and rolled on top of him, causing multiple injuries, including a cut on the head and broken ribs. He was not wearing a helmet.

Frank, who was described as very safety conscious, managed to survive the rollover but the blunt trauma he suffered was too much in the end.

The following recommendations were made after Frank’s death:

- Farmers and other outdoor workers should conduct a thorough evaluation of the terrain to identify hazards prior to operating any offroad vehicle, including ATVs. Frank was aware of the terrain, but misjudged the impact that the

small tree would have on the ATV.

- Farmers (and other employers) should select an off-road utility vehicle equipped with a rollover protective structure (ROPS) and a seatbelt.
 - Operators of off-road utility vehicles should wear a helmet and follow the basic ATV Safety Code.
-

ATV Safety and Gear Fatality File – Spanish

Un granjero muere dos semanas después de volcar en ATV

Frank aguantó “hasta que las vacas volvieron a casa”, pero al final no pudo negociar con un coágulo de sangre.

Este agricultor de Wisconsin, de 66 años, murió dos semanas después de que su vehículo todo terreno (ATV) se le echara encima mientras arreglaba una valla. La semana en que iba a recibir el alta hospitalaria, falleció inesperadamente al levantarse de la cama. La causa de la muerte fue una insuficiencia respiratoria debida a una embolia pulmonar (coágulo de sangre).

La investigación

Según la investigación, Frank había terminado de arreglar una valla dañada por un temporal de viento. Conducía su quad lentamente colina abajo cuando intentó maniobrar sobre un pequeño árbol que crecía de un tocón. Frank supuso que los neumáticos del quad aplastarían el árbol, pero no fue así. En lugar de ello, la máquina volcó, haciéndole caer por un terraplén de seis metros. El quad siguió a Frank colina abajo y rodó sobre él, causándole múltiples heridas, entre ellas un corte en la cabeza y costillas

rotas. No llevaba casco.

Frank, que se describía como una persona muy concienciada con la seguridad, consiguió sobrevivir al vuelco, pero el traumatismo contuso que sufrió fue demasiado al final.

Tras la muerte de Frank se hicieron las siguientes recomendaciones:

- Los agricultores y otros trabajadores al aire libre deben realizar una evaluación exhaustiva del terreno para identificar los peligros antes de manejar cualquier vehículo todoterreno, incluidos los ATV. Frank conocía el terreno, pero calculó mal el impacto que tendría el pequeño árbol en el quad.
- Los agricultores (y otros empresarios) deben elegir un vehículo utilitario todoterreno equipado con una estructura de protección contra vuelcos (ROPS) y un cinturón de seguridad.
- Los conductores de vehículos utilitarios todoterreno deben llevar casco y respetar las normas básicas de seguridad para vehículos todoterreno.

ATV Safety and Gear Infographic



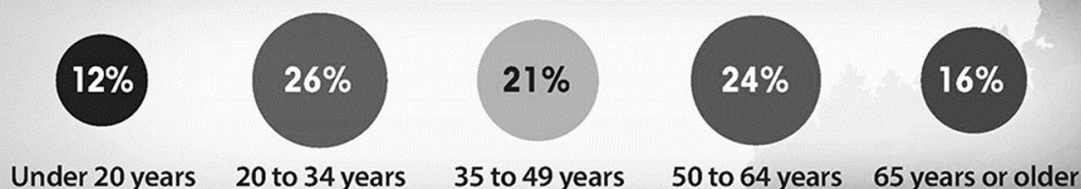
All-terrain vehicle fatalities in Canada, 2013 to 2019¹

On average, **100** all-terrain vehicle (ATV)² fatalities occur every year in Canada.

The vast majority of victims were males.

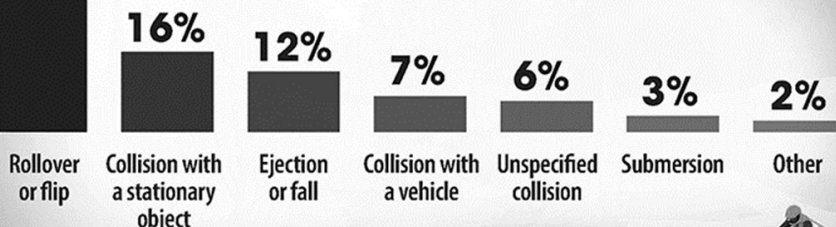
→ **85%** Male **15%** Female

ATV fatalities affected all age groups.



45%

45% of fatalities involved a rollover or flip.³



Risk factors⁴

- **Alcohol/drug use** was reported in **51%** of ATV driver fatalities.
- **Road conditions**, such as a dangerous surface, a slope or a curve, were reported in **33%** of ATV fatalities.
- **Not wearing a helmet/not safely wearing a helmet** was reported in **33%** of ATV fatalities.



ATV Safety and Gear Infographic – Spanish



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.

Maritime Cyber Security Meeting Kit

WHAT'S AT STAKE

Maritime cyber security refers to the protection of information technology systems, networks, and data within the maritime industry from cyber threats. It involves implementing measures and practices to safeguard ships, shore-based infrastructure, communication networks, port systems, and the international supply chain from potential cyberattacks.

WHAT'S THE DANGER

KEY DANGERS ASSOCIATED WITH MARITIME CYBER SECURITY

- Cyberattacks can disrupt maritime operations, if critical systems on a ship are compromised by disrupt navigation, cargo handling, communication.
- Cyber threats can impact the functioning of safety-critical systems, such as fire suppression, emergency response, and life-saving equipment, putting lives at risk.
- Hackers compromise systems controlling ballast water management or fuel transfer operations which lead to pollution incidents, such as accidental discharge of harmful substances into the water.
- Cyber attackers may exploit vulnerabilities in port systems or supply chain processes to gain unauthorized access to cargo information or tamper with shipping documents, leading to potential loss, theft, or compromised supply chain integrity.
- A successful cyberattack can result in the theft or unauthorized access of intellectual property, compromising

competitiveness, trade secrets, and intellectual property rights.

- Maritime systems store and transmit sensitive information, including personal data, financial records, and confidential business information. A data breach or privacy violation can lead to reputational damage, regulatory penalties, and legal liabilities.
- A cyberattack targeting port systems, logistics providers, or shipping companies can disrupt global trade, delay cargo movements, and create economic impacts beyond the maritime sector.
- Maritime cyber security threats may engage in cyber espionage, sabotage, or other malicious activities to gain geopolitical advantages or disrupt critical infrastructure.
- Insufficient cyber insurance coverage within the maritime industry can pose challenges in recovering financial losses incurred due to cyber incidents.

HOW TO PROTECT YOURSELF

TO EFFECTIVE MEASURES TO ADDRESS MARITIME CYBER SECURITY

- Conduct a thorough assessment of potential vulnerabilities and risks within maritime systems, networks, and infrastructure. Identify critical assets, assess their value, and determine the potential impact of cyber threats on operations, safety, and security.
- Create a cybersecurity strategy encompass policies, procedures, and guidelines to mitigate risks and protect against cyber threats.
- Deploy a range of technical and organizational security measures that include firewalls, intrusion detection systems, encryption, secure configurations, access controls, and regular security updates.
- Foster a culture of cybersecurity awareness and promote responsible behavior regarding data protection, password management, and phishing prevention.
- Develop a well-defined incident response plan that outlines procedures for incident detection, containment, analysis,

recovery, and communication.

- Establish forums or platforms for sharing information, threat intelligence, best practices, and lessons learned to stay ahead of evolving cyber threats.
- Ensure compliance with international and regional cybersecurity frameworks to meet minimum security requirements and maintain the trust of stakeholders.
- Implement vendor management practices that include security requirements, audits, and contractual obligations to minimize supply chain risks.
- Regularly conduct vulnerability assessments, penetration testing, and security audits to identify weaknesses and address them promptly.
- Encourage reporting of suspicious activities, provide channels for reporting incidents, and reward proactive cybersecurity practices.
- Leverage advancements in technologies such as artificial intelligence, machine learning, and behavioral analytics to enhance threat detection and response capabilities.
- Regularly review and update security measures, policies, and procedures to address new threats and vulnerabilities.

BEST WORKER MARITIME CYBER SECURITY PRACTICES

- Start by educating yourself about the fundamentals of maritime cyber security. Read books, articles, and industry publications on the subject.
- Follow reputable sources, industry blogs, and news outlets that cover cybersecurity and maritime technology to stay abreast of emerging threats and mitigation strategies.
- Consider pursuing training and certification programs focused on maritime cyber security.
- Attend conferences, seminars, and webinars related to maritime cyber security.
- Join professional networks and online communities dedicated to maritime cyber security.
- Establish personal best practices for maritime cyber security, such as strong password management, regular software updates, being cautious of phishing emails, and

ensuring the security of your personal devices.

- Engage in self-study, online courses, webinars, or workshops to deepen your understanding of emerging technologies and evolving cyber threats.
- Actively participate in information sharing initiatives. Join forums, mailing lists, or online platforms where professionals discuss maritime cyber security.
- Consider finding a mentor who can provide guidance and share their expertise in maritime cyber security.

FINAL WORD

By prioritizing cyber resilience and adopting proactive security measures, the maritime industry can enhance its ability to protect against cyber threats and maintain safe and efficient operations.

Maritime Cyber Security Stats and Facts

FACTS

Scenarios Where Injuries Can Occur Due to Maritime Cyber Incidents

1. A ship's navigation system is compromised through a cyberattack and leads to incorrect or manipulated navigational data resulting in collisions with other vessels, grounding, or incidents involving maritime infrastructure like bridges or offshore structures.
2. Cyberattacks targeting a ship's engine or machinery systems can cause engine failures, propulsion system malfunctions, or loss of power can lead to accidents and injuries.
3. Cyber incidents that disrupt communication systems,

including ship-to-ship, ship-to-shore, or emergency communication channels, can hinder effective coordination and response during critical situations.

4. If maritime vessels' safety systems, such as fire suppression, alarm systems, and emergency response mechanisms, are compromised through cyberattacks, it impairs functionality, potentially leading to delayed or inadequate responses to safety incidents and increasing the risk of injuries.
5. Cyber incidents targeting access control systems, such as electronic locks, security cameras, or entry control mechanisms, result in unauthorized access to sensitive areas of a vessel or maritime facility.

STATS

- Three-quarters of maritime professionals believe a cyber incident is likely to force the closure of a strategic waterway (76%). More than half expect cyber-attacks to cause ship collisions (60%), groundings (68%), and even result in physical injury or death (56%) as an overwhelming majority (79%) of professionals say the industry considers cyber security risks to be as important as health and safety risks.
 - According to the survey, barely 3 in 10 (31%) maritime professionals believe that organizations within their sector are effective at sharing information and lessons learned about cyber security risks, threats, and incidents.
- On the cyber security front, 2021 was not a good year for the maritime and logistics industry. Attacks targeting ships increased in frequency by 33 percent – and that came on the heels of a 900-percent increase in attacks against ships and port systems in 2020.
- In a 2020 Safety at Sea and BIMCO Maritime Cyber Security survey, despite the majority of respondents (77%) viewing cyber-attacks as a high or medium risk to their organizations, few appear to be prepared for the aftermath

of such an attack. 64% of respondents said their organization has a business continuity plan in place to follow in the event of a cyber incident, but only 24% claimed it was tested every three months, and only 15% said that it was tested every six to 12 months. Only 42% of respondents said that their organization protects vessels from operational technology (OT) cyber threats.

Maritime Cyber Security Stats and Facts – Spanish

HECHOS

Escenarios en los que pueden producirse lesiones debido a ciber incidentes marítimos

1. El sistema de navegación de un buque se ve comprometido a través de un ciberataque y da lugar a datos de navegación incorrectos o manipulados que provocan colisiones con otros buques, varadas o incidentes que afectan a infraestructuras marítimas como puentes o estructuras en alta mar.
2. Los ciberataques dirigidos a los sistemas de motor o maquinaria de un buque pueden causar fallos en el motor, mal funcionamiento del sistema de propulsión o pérdida de potencia, lo que puede provocar accidentes y lesiones.
3. Los incidentes cibernéticos que interrumpen los sistemas de comunicación, incluidos los canales de comunicación de buque a buque, de buque a tierra o de emergencia, pueden obstaculizar la coordinación y la respuesta eficaces durante situaciones críticas.
4. Si los sistemas de seguridad de los buques marítimos, como la extinción de incendios, los sistemas de alarma y los mecanismos de respuesta de emergencia, se ven comprometidos

a través de ciberataques, se deteriora su funcionalidad, lo que puede provocar retrasos o respuestas inadecuadas a los incidentes de seguridad y aumentar el riesgo de lesiones.

5. Los incidentes cibernéticos dirigidos contra los sistemas de control de acceso, como cerraduras electrónicas, cámaras de seguridad o mecanismos de control de entrada, dan lugar a un acceso no autorizado a zonas sensibles de un buque o instalación marítima.

ESTADÍSTICAS

- Tres cuartas partes de los profesionales marítimos creen probable que un incidente cibernético obligue a cerrar una vía navegable estratégica (76%). Más de la mitad espera que los ciberataques provoquen colisiones de buques (60%), encallamientos (68%) e incluso provoquen lesiones físicas o la muerte (56%), ya que una abrumadora mayoría (79%) de los profesionales afirma que el sector considera que los riesgos de ciberseguridad son tan importantes como los riesgos para la salud y la seguridad.
 - Según la encuesta, apenas 3 de cada 10 (31%) profesionales marítimos creen que las organizaciones de su sector son eficaces a la hora de compartir información y lecciones aprendidas sobre riesgos, amenazas e incidentes de ciberseguridad.
- En el frente de la ciberseguridad, 2021 no fue un buen año para la industria marítima y logística. La frecuencia de los ataques contra buques aumentó un 33%, tras un aumento del 900% de los ataques contra buques y sistemas portuarios en 2020.
- En una encuesta sobre ciberseguridad marítima realizada por Safety at Sea y BIMCO en 2020, a pesar de que la mayoría de los encuestados (77%) considera los ciberataques como un riesgo alto o medio para sus organizaciones, pocos parecen estar preparados para las consecuencias de un ataque de este tipo. El 64% de los encuestados afirmaron que su organización dispone de un plan de continuidad de la actividad que debe seguirse en caso de incidente

cibernético, pero sólo el 24% afirmó que se ponía a prueba cada tres meses, y sólo el 15% afirmó que se ponía a prueba cada seis a doce meses. Sólo el 42% de los encuestados afirma que su organización protege los buques de las ciberamenazas de la tecnología operativa (OT).

Maritime Cyber Security Fatality File

Port of Houston Breach

In a good example of cyber resilience, the Port of Houston reportedly contained a targeted cyberattack in August 2021, resulting in minimal damage.

From information that was shared, it appears that the incident occurred when cybercriminals exploited a vulnerability in a password manager, to breach the port's network. From there, they attempted to escalate the breach to gain access to other systems.

The Port of Houston's IT team apparently detected the breach quickly, however, and took steps to mitigate it. No sensitive data was exposed, and no systems were apparently disrupted, according to the port (which reported the attack about a month after it occurred and did not release details regarding how long cybercriminals were active or the exact extent of the breach).

Maritime Cyber Security Fatality File – Spanish

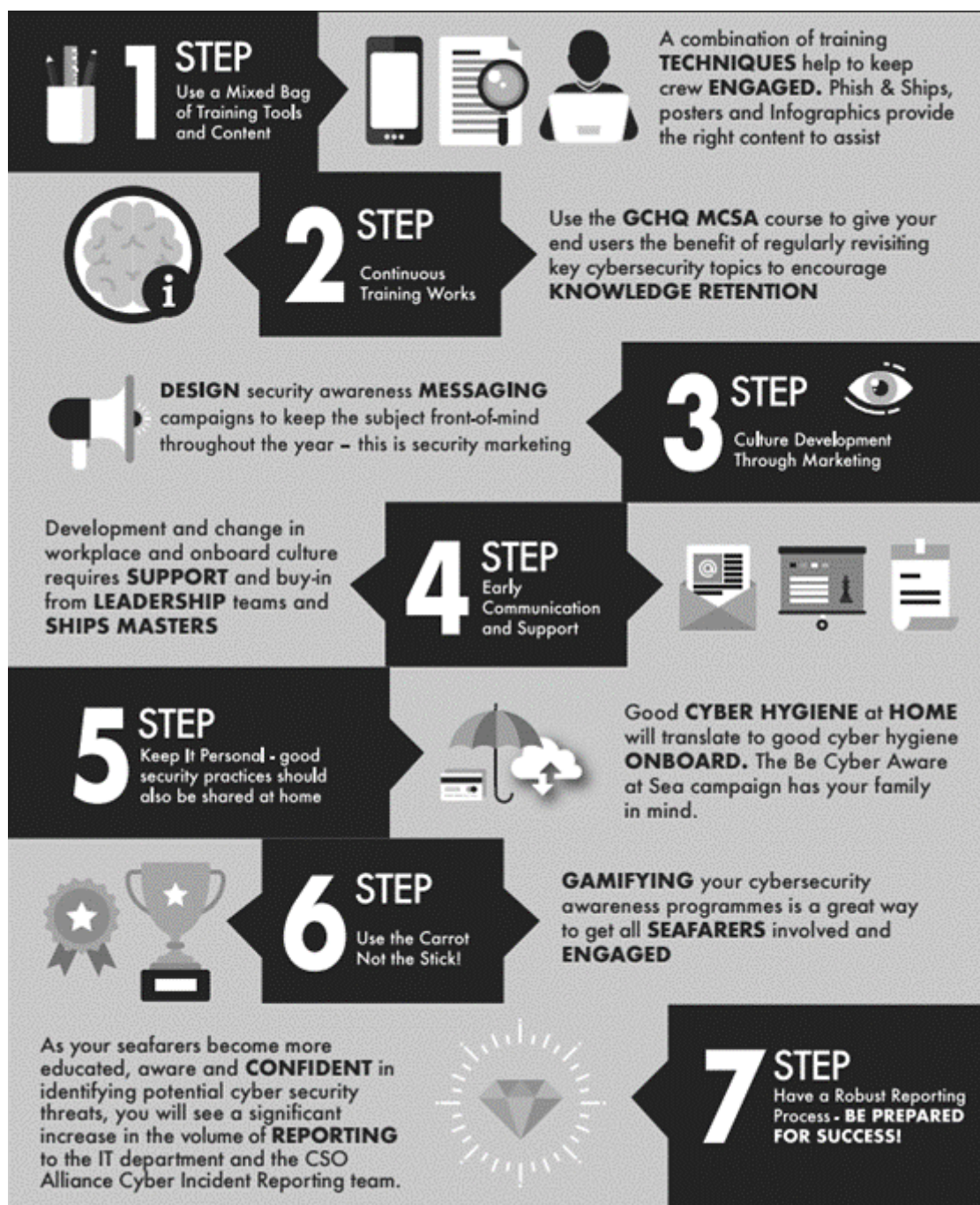
Brecha en el puerto de Houston

En un buen ejemplo de resiliencia cibernética, el Puerto de Houston al parecer contuvo un ciberataque selectivo en agosto de 2021, con el resultado de daños mínimos.

De la información compartida se desprende que el incidente se produjo cuando los ciberdelincuentes aprovecharon una vulnerabilidad en un gestor de contraseñas para acceder a la red del puerto. A partir de ahí, intentaron escalar la brecha para obtener acceso a otros sistemas.

Sin embargo, el equipo informático del puerto de Houston detectó la brecha rápidamente y tomó medidas para mitigarla. Según el puerto (que informó del ataque aproximadamente un mes después de que se produjera y no dio detalles sobre el tiempo que los ciberdelincuentes estuvieron activos o el alcance exacto de la brecha), no se expuso ningún dato sensible ni se interrumpió ningún sistema.

Maritime Cyber Security
Infographic



Source: <https://safety4sea.com>

Maritime Cyber Security Infographic – Spanish

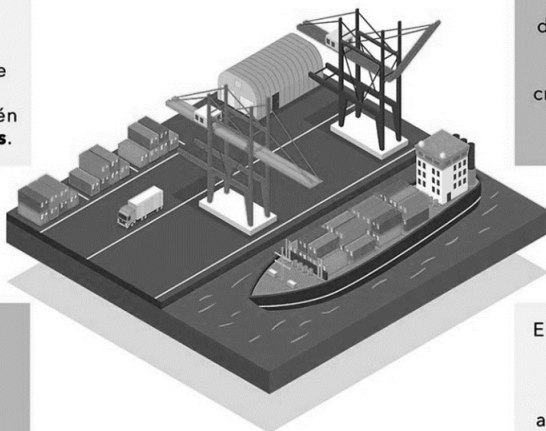


CIBERSEGURIDAD en PUERTOS MARÍTIMOS



Las **instalaciones portuarias** se han ido **conectando a internet**, digitalizando todas sus operaciones. Esto supone muchas innovaciones en sus procesos pero también los hace más **vulnerables**.

Las operaciones de estas instalaciones no pueden detenerse nunca. Por eso, **la ciberseguridad es muy relevante** y debe crecer al mismo ritmo que la implantación de **servicios digitales**.



Como infraestructuras críticas, están en el punto de mira de los cibercriminales y sus sistemas son **objetivo de ciberataques**.

El 80% de los líderes de la industria naviera considera que la ciberseguridad es un asunto **importante o muy importante**, según el informe SMM Maritime Industry Report.



Durante los últimos años se han sucedido diferentes **ataques cibernéticos a puertos**, así como a diversas **empresas de la industria**. Estos han servido para concienciar sobre la importancia que este asunto tiene en los puertos. Aún queda trabajo por hacer. Algunas de las **buenas prácticas a seguir**:



Establecer estrategias y políticas de ciberseguridad adecuadas. El objetivo será aumentar la resistencia cibernética portuaria.

El equipo directivo debe estar involucrado con IT y ciberseguridad. Esto pasa por dedicar un presupuesto adecuado a las medidas de seguridad.

Fuente: <https://globalt4e.com>

Global Maritime Distress and Safety System GMDSS Meeting Kit

WHAT'S AT STAKE

The GMDSS provides a standardized framework for transmitting and receiving distress alerts, maritime safety information, and general communication between ships, search and rescue

authorities, and shore-based facilities.

WHAT'S THE DANGER

RISKS AND CHALLENGES OF GMDSS USAGE

- The GMDSS is susceptible to technical failures, malfunctions, or damage due to harsh marine environments. Equipment failure can hinder distress alerting and communication, delaying rescue.
- The GMDSS is a complex system that requires proper training and knowledge to operate effectively. Ship crews must be trained in the correct use of GMDSS equipment, understanding distress procedures, and interpreting distress messages. Inadequate training or human error can lead to communication errors, incorrect distress alerts, or misinterpretation of distress signals.
- False alerts and hoax calls can divert valuable resources, such as rescue vessels or aircraft, from genuine emergencies. Misuse of GMDSS equipment can put lives at risk and delay assistance for those in real distress.
- There may still be areas with limited or no communication infrastructure, particularly in remote regions or far from shore. Ships face challenges in establishing reliable communication during emergencies.
- Language barriers or differences in procedures and protocols can sometimes create challenges in efficient communication and coordination during distress situations.

HOW TO PROTECT YOURSELF

WHY GMDSS IS CRUCIAL

- The GMDSS provides a standardized and efficient means of communication during distress situations at sea. It ensures that vessels in distress can quickly and effectively transmit distress alerts and communicate their situation to search and rescue authorities, nearby vessels, and coastal stations.

- The GMDSS facilitates the coordination of search and rescue operations. It enables efficient communication between distressed vessels, search and rescue authorities, and other vessels in the vicinity.
- The GMDSS is designed to provide coverage across the world's oceans, even in remote or isolated areas.
- The GMDSS enhances overall safety at sea through the broadcast of navigational warnings, weather forecasts, and other safety-related information. GMDSS enables mariners to stay updated on potential hazards and make informed decisions to mitigate risks.
- GMDSS ensures interoperability between different vessels, search and rescue authorities, and communication systems. Standardization simplifies distress communication procedures, reduces confusion during emergencies, and allows for efficient collaboration among various stakeholders involved in distress response.

BEST WORKER PRACTICES IN GMDSS OPERATIONS

- Obtain the necessary training and certifications to operate GMDSS equipment proficiently.
- Pay close attention to details, particularly when it comes to distress communication and reporting. Small errors can have significant consequences during emergencies.
- Practice clear and concise radio communication, using standard GMDSS phraseology.
- Acquire proficiency in English, which is the international language of maritime communication. Knowledge of other commonly spoken languages among seafarers can be advantageous.
- Be proactive in maintaining and testing GMDSS equipment. Conduct regular checks to ensure the proper functioning of radios, beacons, and other communication devices.
- Participate in training programs, workshops, and industry conferences to expand your knowledge and skills.
- Recognize the importance of teamwork and collaboration in GMDSS operations.
- Develop effective stress management techniques to cope with

the high-pressure situations that can arise during distress incidents. By remaining calm, you can contribute to a more efficient response and help instill confidence in your crew and others involved.

- Uphold high ethical standards and professional integrity in all aspects of your work. Maintain confidentiality of distress information and handle distress calls and communications with sensitivity and professionalism.
- Regularly evaluate your performance and seek feedback from superiors, colleagues, and industry experts.

KEY TOOLS USED IN THE GMDSS OPERATIONS

- **VHF Radio:** Very High Frequency (VHF) radios are widely used for short-range ship-to-ship and ship-to-shore communication.
- **MF/HF Radio:** Medium Frequency (MF) and High Frequency (HF) radios provide long-range communication capabilities for ships at sea.
- **Inmarsat Satellite Communication:** It enables global communication coverage, allowing ships to transmit distress alerts, make voice calls, and send/receive data even in remote areas.
- **Emergency Position Indicating Radio Beacon (EPIRB):** They provide accurate position information to search and rescue authorities, enabling prompt response and assistance.
- **Search and Rescue Transponder (SART):** They transmit radar signals, which are displayed on nearby ships' radar screens, assisting in search and rescue operations.
- **Navtex Receiver:** Navtex is a system that broadcasts maritime safety information, navigational warnings, weather forecasts, and other important messages to ships.
- **Portable VHF Radio:** Portable VHF radios serve as backup communication devices and are easily carried by crew members during emergencies or when leaving the vessel.
- **Digital Selective Calling (DSC):** It allows vessels to send automated distress alerts and position information to nearby ships and shore stations, improving the efficiency of distress communication.

FINAL WORD

The GMDSS plays a critical role in maritime safety by providing a comprehensive system for distress communication, search and rescue coordination, and the dissemination of safety information.

Global Maritime Distress and Safety System GMDSS Meeting Kit – Spanish

QUÉ ESTÁ EN RIESGO

El SMSSM proporciona un marco normalizado para la transmisión y recepción de alertas de socorro, información sobre seguridad marítima y comunicación general entre buques, autoridades de búsqueda y salvamento e instalaciones en tierra.

CUÁL ES EL PELIGRO

RIESGOS Y DESAFÍOS DEL USO DEL SMSSM

- El SMSSM es susceptible de sufrir fallos técnicos, averías o daños debidos a los duros entornos marinos. Los fallos de los equipos pueden dificultar la alerta y la comunicación de socorro, retrasando el rescate.
- El SMSSM es un sistema complejo que requiere capacitación y conocimientos adecuados para funcionar eficazmente. Las tripulaciones de los buques deben recibir capacitación sobre el uso correcto de los equipos del SMSSM, la comprensión de los procedimientos de socorro y la interpretación de los mensajes de socorro. Una capacitación inadecuada o un error

humano pueden provocar errores de comunicación, alertas de socorro incorrectas o una interpretación errónea de las señales de socorro.

- Las alertas falsas y las llamadas de broma pueden desviar recursos valiosos, como buques o aviones de rescate, de emergencias auténticas. El uso indebido de los equipos del SMSSM puede poner en peligro vidas humanas y retrasar la asistencia a las personas en verdadera situación de peligro.
- Todavía puede haber zonas con infraestructuras de comunicación limitadas o inexistentes, sobre todo en regiones remotas o alejadas de la costa. Los buques se enfrentan a dificultades para establecer una comunicación fiable durante las emergencias.
- Las barreras lingüísticas o las diferencias en los procedimientos y protocolos pueden a veces crear dificultades para una comunicación y coordinación eficaces en situaciones de socorro.

COMO PROTEGERSE

POR QUÉ ES CRUCIAL EL SMSSM

- Proporciona un medio de comunicación normalizado y eficaz en situaciones de socorro en el mar. Garantiza que los buques en peligro puedan transmitir rápida y eficazmente alertas de socorro y comunicar su situación a las autoridades de búsqueda y salvamento, a los buques cercanos y a las estaciones costeras.
- Facilita la coordinación de las operaciones de búsqueda y salvamento. Permite una comunicación eficaz entre los buques en apuros, las autoridades de búsqueda y salvamento y otros buques cercanos.
- Está diseñado para proporcionar cobertura en todos los océanos del mundo, incluso en zonas remotas o aisladas.
- Mejora la seguridad general en el mar mediante la difusión de avisos de navegación, previsiones meteorológicas y otras informaciones relacionadas con la seguridad. El SMSSM permite a los navegantes mantenerse al corriente de los peligros potenciales y tomar decisiones con conocimiento de

causa para mitigar los riesgos.

- Garantiza la interoperabilidad entre distintos buques, autoridades de búsqueda y salvamento y sistemas de comunicación. La normalización simplifica los procedimientos de comunicación de socorro, reduce la confusión durante las emergencias y permite una colaboración eficaz entre las diversas partes interesadas que participan en la respuesta de socorro.

MEJORES PRÁCTICAS DE LOS TRABAJADORES EN LAS OPERACIONES DE LA SMSSM

- Obtenga la capacitación y las certificaciones necesarias para manejar con destreza los equipos del SMSSM.
- Preste especial atención a los detalles, sobre todo en lo que se refiere a la comunicación e información de socorro. Los pequeños errores pueden tener consecuencias importantes durante las emergencias.
- Practique una comunicación por radio clara y concisa, utilizando la fraseología estándar del SMSSM.
- Dominar el inglés, que es la lengua internacional de comunicación marítima. Puede ser ventajoso el conocimiento de otros idiomas comúnmente hablados entre la gente de mar.
- Ser proactivo en el mantenimiento y las pruebas de los equipos del SMSSM. Realice comprobaciones periódicas para garantizar el correcto funcionamiento de radios, balizas y otros dispositivos de comunicación.
- Participe en programas de capacitación, talleres y conferencias del sector para ampliar sus conocimientos y habilidades.
- Reconozca la importancia del trabajo en equipo y la colaboración en las operaciones del SMSSM.
- Desarrolle técnicas eficaces de gestión del estrés para hacer frente a las situaciones de gran presión que pueden surgir durante los incidentes de socorro. Manteniendo la calma, puede contribuir a una respuesta más eficaz y ayudar a infundir confianza en su tripulación y en los demás implicados.
- Mantenga altos niveles de ética e integridad profesional en

todos los aspectos de su trabajo. Mantenga la confidencialidad de la información de socorro y gestione las llamadas y comunicaciones de socorro con sensibilidad y profesionalidad.

- Evalúe periódicamente su rendimiento y solicite la opinión de sus superiores, colegas y expertos del sector.

HERRAMIENTAS CLAVE UTILIZADAS EN LAS OPERACIONES DEL SMSSM

- **Radio VHF:** Las radios de muy alta frecuencia (VHF) se utilizan ampliamente para las comunicaciones de corto alcance de barco a barco y de barco a tierra.
- **Radio MF/HF:** Las radios de Media Frecuencia (MF) y Alta Frecuencia (HF) proporcionan capacidades de comunicación de largo alcance para los buques en el mar.
- **Comunicación por satélite Inmarsat:** Permite una cobertura de comunicación global, permitiendo a los buques transmitir alertas de socorro, realizar llamadas de voz y enviar/recibir datos incluso en zonas remotas.
- **Radiobaliza indicadora de posición de emergencia (EPIRB):** Proporcionan información precisa sobre la posición a las autoridades de búsqueda y salvamento, lo que permite una respuesta y asistencia rápidas.
- **Transpondedor de búsqueda y salvamento (SART):** Transmiten señales de radar, que se muestran en las pantallas de radar de los buques cercanos, ayudando en las operaciones de búsqueda y salvamento.
- **Receptor Navtex:** Navtex es un sistema que transmite a los buques información sobre seguridad marítima, avisos de navegación, previsiones meteorológicas y otros mensajes importantes.
- **Radio VHF portátil:** Las radios VHF portátiles sirven como dispositivos de comunicación de reserva y son fácilmente transportables por los miembros de la tripulación durante emergencias o al abandonar el buque.
- **Llamada selectiva digital (DSC):** Permite a los buques enviar alertas de socorro automatizadas e información sobre la posición a los buques y estaciones costeras cercanos, mejorando la eficacia de las comunicaciones de socorro.

CONCLUSIÓN

El SMSSM desempeña un papel fundamental en la seguridad marítima al proporcionar un sistema completo de comunicación de socorro, coordinación de búsqueda y salvamento y difusión de información sobre seguridad.

Global Maritime Distress and Safety System GMDSS Stats and Facts

FACTS

POTENTIAL HAZARDS OF GMDSS

1. False alarms or unintentional activations of distress beacons (such as EPIRBs) can occur. These false alarms can divert resources and cause unnecessary risks for search and rescue teams.
2. Radio communication systems used in the GMDSS, such as VHF, MF/HF, and satellite communication, can be susceptible to interference by atmospheric conditions, electromagnetic interference, or physical obstacles, leading to poor signal quality or disrupted communications.
3. Equipment failures, such as radio malfunctions or satellite system outages, can occur. If onboard equipment fails, it can impede the ship's ability to communicate distress signals or receive assistance promptly.
4. Lack of training or human error can lead to improper use of the GMDSS and potentially compromise safety.
5. Disruption of GMDSS infrastructures, such as power outages

or satellite failures, can hinder the system's effectiveness and delay the response to distress situations.

6. While the GMDSS aims to provide global coverage, there may be areas with limited or no communication coverage, especially in remote or polar regions.

STATS

- It is estimated that with the introduction of GMDSS the safety of life at sea was improved by more than 85%.
- Over 1,500 people lost their lives when radio calls for help to ships in the vicinity went unanswered.
- According to recent IMO statistics, 80% of accidents occurring at sea are caused by human errors, with half due to poor communication.
- Over 1,500 people lost their lives when radio calls for help to ships in the vicinity went unanswered.
- Analysis of the resulting casualty reports determined that radio communications are a prevalent causal factor in marine casualties, being a factor in 18 % of critical vessel casualties, 28 % of critical personnel injuries, and contributing to 19 % of critical marine casualties overall.
- Poor radio communication has been a main contributing factor in numerous maritime casualties, varying from groundings and collisions to entire ship losses and even worse, fatalities. There were 3 accidents in the years 2018 and 2019.

Global Maritime Distress and Safety System GMDSS Stats and Facts – Spanish

HECHOS

PELIGROS POTENCIALES DE LA GMDSS

1. Pueden producirse falsas alarmas o activaciones involuntarias de las balizas de socorro (como las EPIRB). Estas falsas alarmas pueden desviar recursos y causar riesgos innecesarios para los equipos de búsqueda y rescate.
2. Los sistemas de radiocomunicación utilizados en el SMSSM, como las comunicaciones VHF, MF/HF y por satélite, pueden ser susceptibles de sufrir interferencias por las condiciones atmosféricas, interferencias electromagnéticas u obstáculos físicos, lo que provoca una mala calidad de la señal o la interrupción de las comunicaciones.
3. Pueden producirse fallos en los equipos, como averías en las radios o en los sistemas de satélite. Si el equipo de a bordo falla, puede impedir la capacidad del buque para comunicar señales de socorro o recibir ayuda con prontitud.
4. La falta de capacitación o los errores humanos pueden conducir a un uso inadecuado del SMSSM y comprometer potencialmente la seguridad.
5. La interrupción de las infraestructuras del SMSSM, como los cortes de electricidad o los fallos de los satélites, pueden obstaculizar la eficacia del sistema y retrasar la respuesta a las situaciones de socorro.
6. Aunque el SMSSM pretende proporcionar una cobertura mundial, puede haber zonas con una cobertura de comunicaciones limitada o inexistente, especialmente en regiones remotas o polares.

ESTADÍSTICAS

- Se calcula que con la introducción del SMSSM la seguridad de la vida en el mar mejoró en más de un 85%.
- Más de 1.500 personas perdieron la vida cuando las llamadas de socorro por radio a los buques cercanos quedaron sin respuesta.
- Según estadísticas recientes de la OMI, el 80% de los

accidentes que se producen en el mar están causados por errores humanos, y la mitad se deben a una comunicación deficiente.

- Más de 1.500 personas perdieron la vida al quedar sin respuesta las llamadas de socorro por radio a los buques cercanos.
 - El análisis de los informes de siniestros resultantes determinó que las comunicaciones por radio son un factor causal prevalente en los siniestros marítimos, siendo un factor en el 18 % de los siniestros críticos de buques, el 28 % de las lesiones críticas del personal y contribuyendo al 19 % de los siniestros marítimos críticos en general.
 - La mala comunicación por radio ha sido un factor principal que ha contribuido a numerosos siniestros marítimos, que varían desde encallamientos y colisiones hasta pérdidas de buques enteros y, lo que es peor, víctimas mortales. Hubo 3 accidentes en los años 2018 y 2019.
-

Global Maritime Distress and Safety System GMDSS Fatality File

Improper Communication Leads to Accidents At Sea

A vessel was transiting Suez Canal with a pilot onboard where she was supposed to be navigating along the center line of the channel, however as she drifted away from the center line the pilots and bridge team used corrective helms and engines to counter it.

By the time the vessel had swung considerably, and it neared another bank on the opposite side. The stern of the vessel brushed and contacted with a rocky bottom.

A heavy thud was heard and vibrations were felt in the wheelhouse and engine room as well.

The speed of the vessel dropped and picked up again. All ship staff noticed the vibrations. The engine room called up the bridge to confirm if everything was in order.

Both the officers on watch confirmed with the pilot if everything was to which the pilot responded affirmatively.

The vessel had picked up speed again and resumed the canal transit.

The senior officer on watch neither called the master nor discussed it later on with him.

However, below the waterline, the forward part of the hull suffered damages and thus her strength was reduced considerably in the area of impact.

Slight deformation was there but below the waterline. The vessel crossed the canal and while she was loading in the load port, a large thud was heard again, and the officer on watch noticed water rushing in ballast tanks No. 1,2,3 on the Port Side.

Due to continual stresses on a damaged, deformed, and fatigued hull, the weak zone crumbled and gave away.

Global Maritime Distress and

Safety System GMDSS Fatality File -Spanish

Una comunicación inadecuada provoca accidentes en el mar

Un buque que transitaba por el Canal de Suez con un práctico a bordo se suponía que navegaba por la línea central del canal, sin embargo, a medida que se desviaba de la línea central, los prácticos y el equipo del puente utilizaron timones correctivos y motores para contrarrestarlo.

Cuando el buque se había desviado considerablemente, se acercó a otro banco en el lado opuesto. La popa del buque rozó y contactó con un fondo rocoso.

Se oyó un fuerte golpe y también se sintieron vibraciones en el puente de mando y en la sala de máquinas.

La velocidad del buque disminuyó y volvió a aumentar. Todo el personal del buque notó las vibraciones. La sala de máquinas llamó al puente para confirmar si todo estaba en orden.

Los dos oficiales de guardia confirmaron con el piloto si todo estaba en orden, a lo que el piloto respondió afirmativamente.

El buque había recuperado la velocidad y reanudó el tránsito por el canal.

El oficial superior de guardia no llamó al capitán ni lo discutió posteriormente con él.

Sin embargo, por debajo de la línea de flotación, la parte delantera del casco sufrió daños, por lo que su resistencia se redujo considerablemente en la zona del impacto.

Había una ligera deformación, pero por debajo de la línea de flotación. El buque cruzó el canal y mientras cargaba en el puerto

de carga, se oyó de nuevo un gran estruendo, y el oficial de guardia notó que corría agua en los tanques de lastre nº 1,2,3 del costado de babor.

Debido a las continuas tensiones en un casco dañado, deformado y fatigado, la zona débil se desmoronó y cedió.

Global Maritime Distress and Safety System GMDSS Infographic

Global Maritime Distress and Safety System

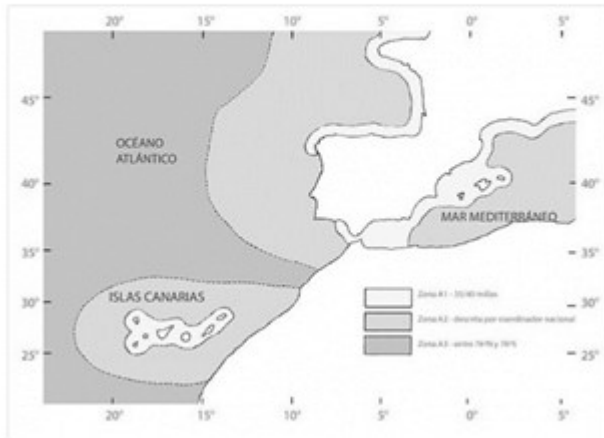
Ships at sea must be capable of the following functional GMDSS requirements:

1. Ship-to-shore distress alerting.
2. Shore-to-ship distress alerting.
3. Ship-to-ship distress alerting.
4. SAR coordination.
5. On-scene communications.
6. Transmission and receipt of emergency locating signals.
7. Transmission and receipt of MSI.
8. General radio communications.
9. Bridge-to-bridge communications.

Source: <https://ppt-online.org>

Global Maritime Distress and Safety System GMDSS Infographic – Spanish

¿QUÉ ZONAS DE NAVEGACIÓN CUBRE EL SMSSM?



En el SMSSM existen 4 zonas de cobertura radioeléctrica para cubrir todas las zonas marítimas del mundo, las cuales se encuentran definidas por el grado de cobertura. Estas zonas son:

- Zona A1: zona comprendida en el ámbito de cobertura VHF de una estación costera, en la que se dispone del alerta de llamada selectiva digital (aproximadamente 35/40 millas).
- Zona A2: zona comprendida en el ámbito de cobertura MF de una estación costera, en la que se dispone del alerta de llamada selectiva digital. En España es la que ha definido el coordinador nacional para cada transmisor NAVTEX.
- Zona A3: excluyendo las Zonas 1 y 2, es el área de cobertura de la onda corta y de la red de satélites geostacionarios de INMARSAT, red que abarca hasta los 76° Norte y los 76° Sur.
- Zona A4: Comprende las zonas polares, en las que no existe cobertura de los satélites INMARSAT.

Fuente: <http://www.salvamentomaritimo.es>

Radio Communication – Maritime Safety Meeting Kit

WHAT'S AT STAKE

Radio communication in maritime safety refers to the use of radio systems and procedures to facilitate communication between vessels, maritime authorities, and other relevant parties to ensure the safety of maritime operations.

WHAT'S THE DANGER

DANGERS OF RADIO COMMUNICATION IN MARITIME SAFETY

- Miscommunication can occur due to language barriers, improper use of terminology, unclear or garbled transmissions, or misunderstanding of information.
- Radio signals can be subject to interference from various sources, which can degrade the quality of communication, distort messages, or result in signal loss, making it challenging to transmit or receive important information accurately.
- Poor signal quality, background noise, or weak reception can make it difficult to understand crucial information, instructions, or distress calls accurately and hamper effective responses.
- Radio equipment can experience technical failures or malfunctions, such as transmitter issues, power supply problems, or antenna failures. Leading to communication breakdowns during critical situations.
- Relying solely on radio communication without alternative means, such as visual signals or backup systems, can leave vessels vulnerable in emergencies.
- Insufficient training and lack of familiarity with radio equipment and procedures can lead to ineffective or incorrect use of radio communication.
- Radio communication systems can be vulnerable to unauthorized interception of transmissions which compromise the confidentiality of sensitive information or enable malicious actors to mislead or deceive vessels.

HOW TO PROTECT YOURSELF

KEY STEPS TO DEAL WITH RADIO COMMUNICATION IN MARITIME SAFETY

- Familiarize yourself with the operation of the radio equipment, including controls, channels, and functions.
- When communicating over the radio, use clear and concise language to ensure the message is easily understood. Avoid

jargon, slang, or abbreviations that may confuse you. Speak slowly, enunciate clearly, and maintain a calm and professional tone.

- Utilize standardized phrases and procedures for radio communication by international guidelines and local regulations. Be familiar with common phrases for distress calls, routine messages, navigational instructions, and emergency procedures.
- Practice good radio discipline to ensure effective communication. Listen attentively to other parties before transmitting, avoid unnecessary or prolonged transmissions, and maintain professional conduct.
- Identify yourself and your vessel at the beginning of each transmission. State your vessel's name and call sign, followed by the name or call sign of the vessel or station you are addressing. Introduce the purpose of your communication to ensure clarity and to enable others to respond appropriately.
- Actively listen to incoming messages and respond promptly when required. Acknowledge receipt of messages to confirm understanding and let the sender know you have received their communication.
- In distress situations, follow established distress communication procedures. Use the international distress signal "Mayday" to indicate an immediate threat to the safety of your vessel or its occupants.
- Continuously monitor radio channels and frequencies designated for maritime safety to stay aware of potential safety hazards, navigational warnings, weather updates, or other critical information.
- Keep accurate records of all radio communications. Record the date, time, participants, and the content of each communication.
- If you encounter difficulties or need assistance with radio communication, don't hesitate to seek support.

SKILL SET OF A GOOD RADIO COMMUNICATIONS WORKER IN MARITIME SAFETY

- Acquire a comprehensive understanding of the relevant

international and local regulations, such as those established by the International Maritime Organization (IMO) and your country's maritime authority.

- Seek appropriate training courses and certifications related to radiocommunications and maritime security.
- Familiarize yourself with different types of radios, their functions, controls, and how to troubleshoot common issues. Practice operating radios and communication systems to ensure efficiency.
- Practice clear and concise communication techniques, using proper radio terminology and standard phrases. Speak slowly, enunciate clearly, and maintain a professional tone. Listen actively to understand messages and confirm receipt or understanding when required.
- Stay vigilant and maintain situational awareness by actively monitoring radio channels and frequencies designated for maritime security. Stay informed about ongoing security operations, potential threats, and any relevant safety information or alerts.
- Ensure that sensitive information is not transmitted over open or unsecured radio channels.
- Familiarize yourself with emergency response procedures and be prepared to handle distress calls, emergencies, and security incidents.
- Work closely with other radiocommunications workers and maritime security personnel.
- Maintain accurate records and logs of all radio communications.
- Continuously update your knowledge and skills by staying informed about advancements in radiocommunication technology, regulatory changes, and best practices in maritime security.

FINAL WORD

Radio communication encompasses the transmission and reception of voice, data, and signaling information through radio waves to exchange vital information related to navigational safety,

emergencies, distress calls, and coordination during maritime operations.

Radio Communication – Maritime Safety Meeting Kit – Spanish

QUÉ ESTÁ EN RIESGO

La radiocomunicación en la seguridad marítima se refiere al uso de sistemas y procedimientos de radio para facilitar la comunicación entre buques, autoridades marítimas y otras partes relevantes para garantizar la seguridad de las operaciones marítimas.

CUÁL ES EL PELIGRO

PELIGROS DE LA COMUNICACIÓN POR RADIO EN LA SEGURIDAD MARÍTIMA

- Pueden producirse fallos de comunicación debido a barreras lingüísticas, uso inadecuado de la terminología, transmisiones poco claras o confusas, o malentendidos de la información.
- Las señales de radio pueden estar sujetas a interferencias de diversas fuentes, lo que puede degradar la calidad de la comunicación, distorsionar los mensajes o provocar la pérdida de la señal, dificultando la transmisión o recepción de información importante con precisión.
- La mala calidad de la señal, el ruido de fondo o una recepción débil pueden dificultar la comprensión exacta de información crucial, instrucciones o llamadas de socorro y obstaculizar respuestas eficaces.
- Los equipos de radio pueden sufrir fallos técnicos o averías, como problemas con el transmisor, la fuente de

alimentación o la antena. Esto puede provocar fallos de comunicación en situaciones críticas.

- Depender únicamente de la comunicación por radio sin medios alternativos, como señales visuales o sistemas de reserva, puede dejar a los buques vulnerables en situaciones de emergencia.
- Una capacitación insuficiente y la falta de familiaridad con los equipos y procedimientos de radio pueden conducir a un uso ineficaz o incorrecto de las radiocomunicaciones.
- Los sistemas de comunicación por radio pueden ser vulnerables a la interceptación no autorizada de las transmisiones, lo que compromete la confidencialidad de la información sensible o permite a agentes malintencionados inducir a error o engañar a los buques.

COMO PROTEGERSE

PASOS CLAVE PARA TRATAR LA COMUNICACIÓN POR RADIO EN LA SEGURIDAD MARÍTIMA

- Familiarícese con el funcionamiento del equipo de radio, incluidos los controles, canales y funciones.
- Cuando se comunique por radio, utilice un lenguaje claro y conciso para asegurarse de que el mensaje se entiende fácilmente. Evite jerga, argot o abreviaturas que puedan confundir. Hable despacio, enuncie con claridad y mantenga un tono tranquilo y profesional.
- Utilice frases y procedimientos estandarizados para la comunicación por radio según las directrices internacionales y la normativa local. Familiarícese con las frases comunes para llamadas de socorro, mensajes de rutina, instrucciones de navegación y procedimientos de emergencia.
- Practique una buena disciplina de radio para garantizar una comunicación eficaz. Escuche atentamente a las otras partes antes de transmitir, evite transmisiones innecesarias o prolongadas y mantenga una conducta profesional.
- Identifíquese a sí mismo y a su embarcación al comienzo de cada transmisión. Indique el nombre y el indicativo de llamada de su barco, seguido del nombre o indicativo de

llamada del barco o estación a la que se dirige. Presente el propósito de su comunicación para garantizar la claridad y permitir que los demás respondan adecuadamente.

- Escuche activamente los mensajes entrantes y responda con prontitud cuando sea necesario. Acuse recibo de los mensajes para confirmar que los ha entendido y haga saber al remitente que ha recibido su comunicación.
- En situaciones de socorro, siga los procedimientos de comunicación de socorro establecidos. Utilice la señal internacional de socorro “Mayday” para indicar una amenaza inmediata para la seguridad de su buque o de sus ocupantes.
- Supervise continuamente los canales de radio y las frecuencias designadas para la seguridad marítima a fin de estar al tanto de posibles peligros para la seguridad, avisos de navegación, actualizaciones meteorológicas u otra información crítica.
- Mantenga registros precisos de todas las comunicaciones por radio. Anote la fecha, la hora, los participantes y el contenido de cada comunicación.
- Si tiene dificultades o necesita ayuda con la comunicación por radio, no dude en pedir ayuda.

CONJUNTO DE APTITUDES DE UN BUEN TRABAJADOR DE RADIOCOMUNICACIONES EN SEGURIDAD MARÍTIMA

- Adquiera un conocimiento exhaustivo de la normativa internacional y local pertinente, como la establecida por la Organización Marítima Internacional (OMI) y la autoridad marítima de su país.
- Busque cursos de capacitación y certificaciones adecuados relacionados con las radiocomunicaciones y la seguridad marítima.
- Familiarícese con los diferentes tipos de radios, sus funciones, controles y cómo solucionar los problemas más comunes. Practique el manejo de radios y sistemas de comunicación para garantizar su eficacia.
- Practique técnicas de comunicación claras y concisas, utilizando la terminología de radio adecuada y frases estándar. Hable despacio, enuncie con claridad y mantenga un

tono profesional. Escuchar activamente para comprender los mensajes y confirmar la recepción o comprensión cuando sea necesario.

- Permanezca alerta y mantenga un conocimiento de la situación supervisando activamente los canales de radio y las frecuencias designadas para la protección marítima. Manténgase informado sobre las operaciones de seguridad en curso, las amenazas potenciales y cualquier información o alerta de seguridad pertinente.
- Asegúrese de que no se transmite información sensible a través de canales de radio abiertos o no seguros.
- Familiarícese con los procedimientos de respuesta a emergencias y esté preparado para atender llamadas de socorro, emergencias e incidentes de seguridad.
- Colabore estrechamente con otros trabajadores de radiocomunicaciones y con el personal de seguridad marítima.
- Mantenga registros y diarios precisos de todas las comunicaciones por radio.
- Actualice continuamente sus conocimientos y aptitudes manteniéndose informado sobre los avances en la tecnología de las radiocomunicaciones, los cambios normativos y las mejores prácticas en materia de protección marítima.

CONCLUSIÓN

La radiocomunicación abarca la transmisión y recepción de voz, datos e información de señalización a través de ondas de radio para intercambiar información vital relacionada con la seguridad de la navegación, las emergencias, las llamadas de socorro y la coordinación durante las operaciones marítimas.

Radio Communication – Maritime Safety Stats and Facts

FACTS

Accidents can occur due to inadequate radio communication:

1. Inadequate communication regarding course changes, passing arrangements, or navigational hazards can lead to vessels inadvertently crossing paths and colliding with each other.
2. If navigational warnings, information about shifting channels, or updates on underwater obstructions are not effectively communicated, vessels may unknowingly enter hazardous areas and run aground.
3. In emergencies, if distress calls or requests for assistance are not effectively transmitted or received due to poor radio communication, the response time of rescue authorities or nearby vessels may be delayed.
4. Inaccurate or unclear communication can lead to incorrect actions, such as improper maneuvering, misjudgment of passing distances, or failure to understand navigational warnings, which can increase the risk of accidents.
5. Inadequate monitoring of radio channels and failure to receive or comprehend safety information broadcasts can result in vessels operating without knowledge of changing weather conditions, navigational hazards, or nearby vessels, increasing the likelihood of accidents.
6. Insufficient communication regarding the handling of hazardous materials or pollution response procedures can result in environmental incidents causing harm to the marine ecosystem.

STATS

- Over 1,500 people lost their lives when radio calls for help to ships in the vicinity went unanswered. Multiple smaller-

scale incidents happen every day across the globe.

- Analysis of the resulting casualty reports determined that radio communications are a prevalent causal factor in marine casualties, being a factor in 18 % of critical vessel casualties, 28 % of critical personnel injuries, and contributing to 19 % of critical marine casualties overall.
- Poor radio communication has been a main contributing factor in numerous maritime casualties, varying from groundings and collisions to entire ship losses and even worse, fatalities. There were 3 accidents in the years 2018 and 2019.
- 392 ships with radio equipment malfunctions with the means of Analysis of Variances (ANOVA) and Chi-square tests. It was found that ships of certain characteristics, such as type and size, frequently have radio communication failures.
- According to recent IMO statistics, 80% of accidents occurring at sea are caused by human errors, with half due to poor communication.