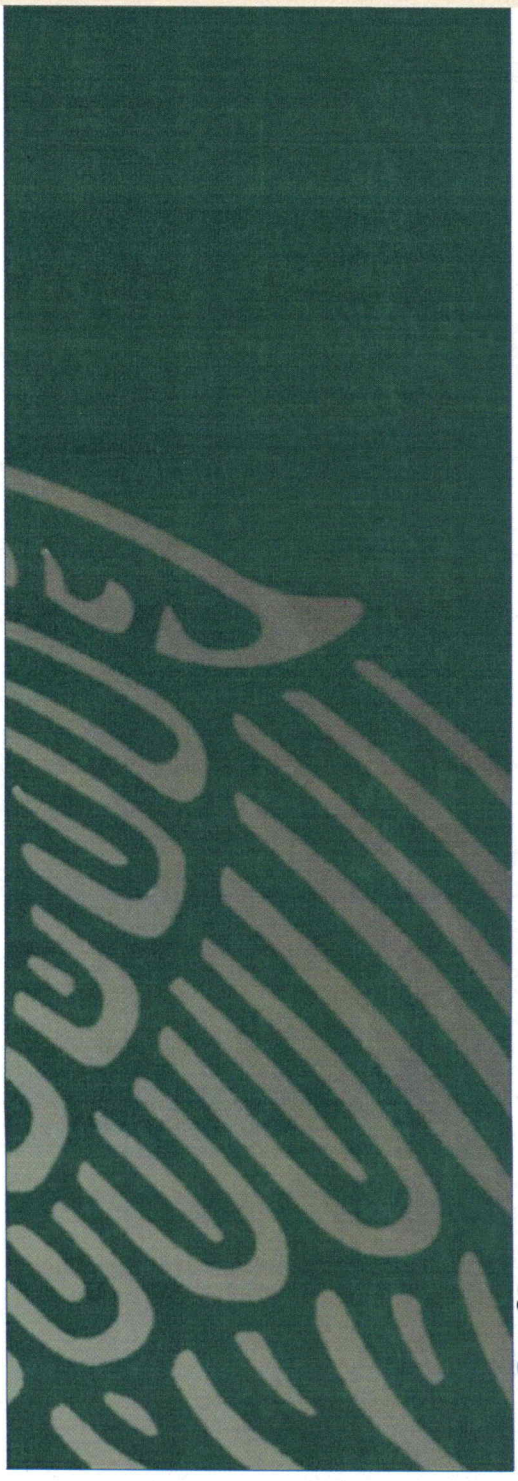
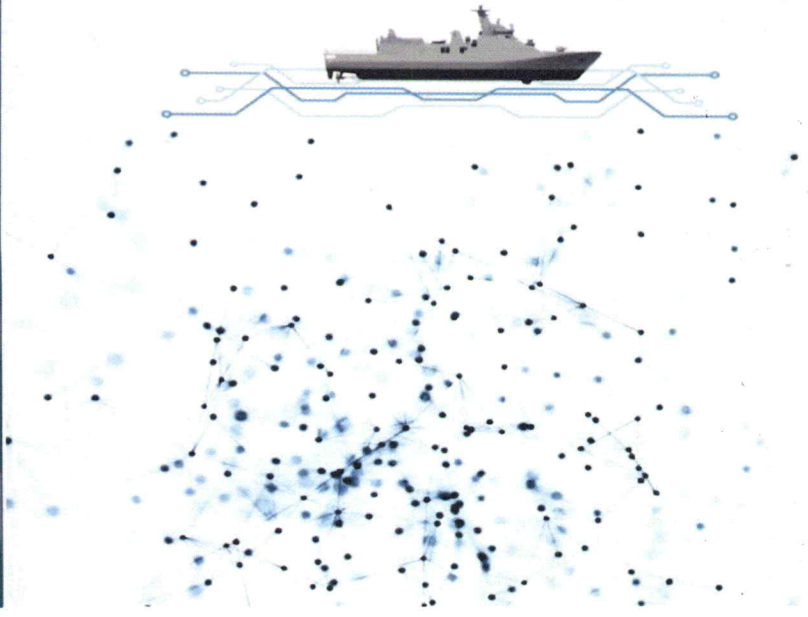
MARINA

SECRETARÍA DE MARINA

ESTRATEGIA INSTITUCIONAL PARA EL CIBERESPACIO 2021-2024





Mensaje del Almirante Secretario de Marina

El desarrollo acelerado de las tecnologías de la información y la comunicación, en un mundo por demás hiperconectado, ha tenido un impacto sin precedentes para todos los sectores de la sociedad, cambiando de manera sustancial la forma de gestionar los ámbitos político, económico, social, diplomático, tecnológico y sin duda, militar; lo que ha derivado en la conformación del ciberespacio como un entorno más para el desarrollo de los Estados-Nación.

Sin embargo, las amenazas emergentes que aprovechan la propia naturaleza de las redes de comunicación actuales, están llevando a cabo acciones que impactan en la seguridad nacional de los países alrededor del mundo, como lo son, la afectación de infraestructuras críticas que proveen bienes y servicios a la sociedad, donde es vital garantizar la continuidad de sus operaciones.

Por este motivo, el Estado mexicano y nuestra Institución le asignan una importancia estratégica desde la creación de la Comisión de Seguridad de la Información en 2004, al preparar profesionalmente recursos humanos a través del Sistema Educativo Naval, en apoyo a las instancias de seguridad nacional.

De esta forma, hemos contribuido en alcanzar y mantener un adecuado nivel de capacidades en materia de seguridad en el Ciberespacio, a pesar de las amenazas tradicionales y emergentes de los últimos años, las cuales demanda de nosotros una reorganización y optimización de los recursos humanos, materiales y financieros, destinados a proporcionar seguridad en este importante ámbito, con el objetivo de coadyuvar, de manera más eficiente, al mantenimiento de la integridad, estabilidad y permanencia de nuestra Nación.

Con la presente estrategia, tenemos el objetivo de coadyuvar de forma más eficiente, al mantenimiento de la integridad, estabilidad y permanencia del Estado mexicano, al disminuir el riesgo institucional en el ámbito marítimo nacional y coadyuvar en el esfuerzo nacional para mantener la continuidad de los servicios críticos que se proporcionan a la sociedad mexicana, a través de las instalaciones estratégicas del país.

Así como desarrollamos proyectos para la construcción de buques, o adquisición de aeronaves, material y equipo para las operaciones de mar, aire y tierra, con la Estrategia Institucional para el Ciberespacio se orientarán los esfuerzos institucionales para fortalecer las capacidades de Ciberdefensa, Ciberseguridad y Seguridad de la Información, en apego a la Estrategia Prioritaria 1.4 del Programa Sectorial de Marina: "Fortalecer las capacidades de seguridad en el Ciberespacio para coadyuvar con la seguridad nacional y la seguridad interior", en alineación con el Plan Nacional de Desarrollo 2019-2024.

En el cumplimiento de las atribuciones institucionales, mediante el empleo del Poder Naval de la Federación, a la par que en el mar, en el aire y en la tierra, la seguridad en el ciberespacio continuará siendo una prioridad para mantener las condiciones de paz bajo un estricto respeto a los Derechos Humanos y el cumplimiento de la legislación nacional e internacional vigentes, a través de la Unidad de Ciberseguridad del Estado Mayor General de la Armada y de los diferentes organismos internos de la Secretaría de Marina-Armada de México.

Ciudad de México, mayo de 2021.

Almirante
José Rafael Ojeda Durán
Secretario de Marina
y Alto Mando de la Armada de México

ÍNDICE

INTRODUCCIÓN

El desconocimiento de los riesgos que conlleva el empleo del Ciberespacio por la mayoría de los sectores de la sociedad, la marcada dependencia tecnológica en la última década, la falta de regulación de este entorno a nivel mundial, así como su fácil acceso bajo el anonimato por cualquier individuo o actor antagónico desde cualquier parte del mundo, aunado a la falta de fronteras físicas como las del territorio, han hecho que las amenazas tradicionales y emergentes encuentren nuevas formas de operar para impactar en la soberanía, integridad, estabilidad y permanencia de los Estados-Nación.

De acuerdo con el informe de riesgos mundiales 2019 del Foro Económico Mundial, los ciberataques están considerados en el quinto lugar en términos de probabilidad y en el séptimo en términos de impacto; señalando que los riesgos asociados con las noticias falsas, robo de identidad e interrupción de operaciones de infraestructuras críticas van en aumento. Los recientes incidentes cibernéticos a nivel mundial han revelado nuevas debilidades de hardware y software, aunado al uso potencial de la Inteligencia Artificial para ingeniar ciberataques más sofisticados, lo que pone en riesgo a las Instalaciones Estratégicas de los Estados y con ello a la sociedad en general; razón por la cual se deben fortalecer las capacidades humanas y tecnológicas por motivos de Seguridad Nacional.

La Organización de Estados Americanos y el Banco Interamericano de Desarrollo, en su reporte "Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe", hizo un balance de esfuerzos realizados en los últimos cuatro años por los países en la región. En escala de 1 a 5, México presentó un nivel de madurez promedio de 2 en las dimensiones de "Cultura y sociedad" y "Educación, capacitación y habilidades", mientras que en las dimensiones "Política y estrategia" y "Estándares, organizaciones y tecnologías" fue inferior a 2; habiendo destacado en la dimensión "Marcos legales y regulatorios" con un nivel de madurez de entre 2 y 3. Aun cuando es uno de los países mejores posicionados en la región, esto no es suficiente para hacer frente a los retos y las amenazas de nivel global en el Ciberespacio.

En los últimos dos años, México ha estado a prueba de estos ciberataques, tanto en infraestructuras críticas del sector industrial como del sector financiero, así como en páginas web y cuentas de redes sociales de Instituciones gubernamentales, con la finalidad de afectar los servicios y la imagen pública del Estado mexicano.

En este contexto, es posible apreciar que nuestro país y particularmente el sector marítimo nacional, no se encuentra libre de amenazas, por el contrario, el nivel de riesgos se incrementa en la medida que dejamos de tomar acciones para anticipar los eventos e incidentes de seguridad en el Ciberespacio.

Proteger nuestra propia infraestructura tecnológica para soportar los procesos críticos de la Institución, como son las Operaciones Navales que se desarrollan por mar, aire y tierra, además de gestionar el Riesgo Cibernético Marítimo y Portuario como Autoridad Marítima Nacional, pone de manifiesto la necesidad de generar líneas de acción a través de la optimización de los recursos humanos, materiales y financieros, a efectos de que los organismos internos coordinen y dirijan los esfuerzos para fortalecer y consolidar las capacidades de Ciberdefensa, Ciberseguridad y Seguridad de la Información.

Por tal motivo, la presente estrategia tiene como propósito, generar las condiciones al interior de la Institución para consolidar la fuerza laboral cibernética, su desarrollo profesional y las operaciones navales en el ciberespacio, para hacer frente a las amenazas y riesgos de Seguridad Nacional desde el entorno marítimo de acuerdo con la Agenda Institucional de Riesgos vigente; de manera que se contribuya al mantenimiento de la integridad, estabilidad y permanencia del Estado Mexicano; que bajo la atribución del Jefe de Estado Mayor de la Armada de México, la Unidad de Ciberseguridad (EMGA-UNICIBER) deberá planear, conducir y ejecutar las líneas de acción descritas en la presente estrategia en colaboración y coordinación con los diferentes organismos internos de la Institución, bajo el estricto respeto a los Derechos Humanos y cumplimiento de la legislación nacional e internacional vigente.

MARCO JURÍDICO NACIONAL

A. Constitución Política de los Estados Unidos Mexicanos.

El artículo 89 fracción VI de la Constitución Política de los Estados Unidos Mexicanos, dispone que es facultad y obligación del Presidente de la República, preservar la seguridad nacional y disponer de la totalidad de la Fuerza Armada permanente o sea del Ejército, de la Armada y de la Fuerza Aérea para la seguridad interior y defensa exterior de la Federación.

B. Ley Orgánica de la Administración Pública Federal.

El Artículo 30 fracciones I y XX, establece que corresponde a la Secretaría de Marina preparar a la Armada, con el fin de ejercer acciones para llevar a cabo la defensa y seguridad nacionales en el ámbito de su responsabilidad.

C. Ley de Seguridad Nacional.

El Artículo 3/o. fracción I, manifiesta que debe entenderse por Seguridad Nacional las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a su protección frente a las amenazas y riesgos que enfrente nuestro país.

El Artículo 5/o fracciones I, V y XII, manifiesta que son amenazas a la Seguridad Nacional, los actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional, obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada, así como destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

D. Ley Orgánica de la Armada de México.

El Artículo 1/o. establece que la misión de la Armada de México es emplear el poder naval de la Federación para la defensa exterior y coadyuvar en la seguridad interior del país.

El Artículo 2/o. fracción II y VI, establece que, entre las atribuciones de la Armada de México, se encuentra cooperar en el mantenimiento del orden constitucional del Estado Mexicano; así como proteger instalaciones estratégicas del país en su ámbito de competencia y donde el Mando Supremo lo ordene.

El Artículo 3/o. enuncia que la Armada de México ejerce sus atribuciones por sí o conjuntamente con el Ejército y Fuerza Aérea cuando lo ordene el Mando Supremo.

E. Reglamento Interior de la Secretaría de Marina.

El Artículo 10 fracción XL, establece que el Jefe de Estado Mayor General de la Armada tiene la facultad de planear, conducir y ejecutar actividades de seguridad y ciberdefensa para la protección de la infraestructura crítica de la Secretaría y coadyuvar en el ámbito de su competencia con las demás instituciones del Estado.

F. Acuerdo Secretarial del Alto Mando número 033 de marzo de 2017.

La misión de la Unidad de Ciberseguridad es planear, conducir y ejecutar actividades de seguridad de la información, ciberseguridad y ciberdefensa, para la protección de la infraestructura crítica de la SEMAR y coadyuvar en el esfuerzo nacional en el mantenimiento de la integridad, estabilidad y permanencia del Estado Mexicano.

G. Plan Nacional de Desarrollo 2019-2024.

Eje 1 Política y Gobierno, línea de acción 9. Repensar la Seguridad Nacional y reorientar a las Fuerzas Armadas. Los soldados y marinos de México son pueblo uniformado. El Gobierno Federal procurará incrementar la confianza de la población civil hacia las Fuerzas Armadas, impulsará la colaboración entre una y las otras y enfatizará el papel de estas como parte de la sociedad. El Ejército Mexicano y la Armada de México conservarán sus tareas constitucionales en la preservación de la seguridad nacional y la integridad territorial del país, la

defensa de la soberanía nacional y a asistencia a la población en casos de desastres; asimismo, los institutos armados seguirán aportando a diversas esferas del quehacer nacional: aeronáutica, informática, industria, ingeniería, entre otras.

H. Programa Sectorial de Marina 2020-2024.

Objetivo prioritario 1. Preservar la seguridad nacional y coadyuvar en la seguridad interior del país, en su estrategia prioritaria 1.4 "fortalecer las capacidades de seguridad en el Ciberespacio para coadyuvar con la seguridad nacional y la seguridad interior", así como el objetivo prioritario 3. Fortalecer la Autoridad Marítima Nacional, en su estrategia 3.2 "Fortalecer las capacidades en materia de protección marítima y portuaria para el mantenimiento del Estado de derecho en aguas nacionales y recintos portuarios".

ALCANCE

La presente Estrategia se plantea como el documento rector en la Secretaría de Marina para que, en el ámbito de sus atribuciones, la Institución fortalezca las capacidades para identificar y hacer frente a las amenazas provenientes del Ciberespacio que puedan afectar a la Institución y el entorno marítimo nacional.

OBJETIVO GENERAL.

Establecer las acciones puntuales de la Secretaría de Marina para materializar la Estrategia prioritaria 1.4 y coadyuvar en la estrategia 3.2 del Programa Sectorial de Marina 2020-2024 que permitan administrar el riesgo cibernético institucional y marítimo nacional.

MISIÓN

Fortalecer las capacidades humanas, tecnológicas, operacionales, normativas, legales y doctrinales, así como promover la coordinación y cooperación tanto en el ámbito interno, como en lo nacional e internacional mediante una fuerza laboral cibernética que desarrolle las operaciones navales de seguridad en el Ciberespacio.

VISIÓN

Ser una Institución referente en materia de seguridad en el Ciberespacio, a través del desarrollo de las capacidades de Ciberdefensa, Ciberseguridad y Seguridad de la Información, mediante operaciones en el Ciberespacio con estricto apego a los derechos humanos, acuerdos y tratados internacionales.

ESTRATEGIAS PRIORITARIAS DEL PROGRAMA SECTORIAL DE MARINA 2020-2024

Estrategia prioritaria 1.4 (EMGA-UNICIBER) Fortalecer las capacidades de seguridad en el ciberespacio para coadyuvar con la seguridad nacional y seguridad interior.

Estrategia prioritaria 3.2 (EMGA-UNICIBER coadyuvante con UNICAPAM en materia de riesgo cibernético marítimo) Fortalecer las capacidades en materia de protección marítima y portuaria para el establecimiento del Estado de Derecho en aguas nacionales y recintos portuarios.

ACCIONES PUNTUALES DE SEGURIDAD EN EL CIBERESPACIO

1. Desarrollar y mantener las capacidades humanas y tecnológicas que apoyen las operaciones en el ciberespacio, fortaleciendo las acciones institucionales en materia de ciberseguridad para el mantenimiento de la integridad y permanencia del Estado Mexicano.
2. Contribuir con el esfuerzo nacional para reducir la vulnerabilidad cibernética, a través de la coordinación y cooperación con otras FF. AA., sector público, privado y académico, a favor de la Seguridad Nacional y Seguridad Interior.
3. Planear, conducir y ejecutar actividades de seguridad de la información, ciberseguridad y ciberdefensa, a través de operaciones en el ciberespacio.
4. Promover el marco jurídico, la normatividad interna y doctrina adecuada en materia de operaciones en el ciberespacio, a fin de actuar conforme a derecho en materia de ciberseguridad.

LÍNEAS DE ACCIÓN ESPECIFICAS

ACCIÓN PUNTUAL UNO

Desarrollar y mantener las capacidades humanas y tecnológicas que apoyen las operaciones en el ciberespacio, fortaleciendo las acciones institucionales en materia de ciberseguridad para el mantenimiento de la integridad y permanencia del Estado Mexicano.

1.1. Optimizar el recurso humano a través de la conformación de la fuerza cibernética laboral en la Secretaría de Marina.

1.2. Concientizar en Seguridad de la Información, Ciberseguridad y Ciberdefensa; generando además la memoria histórica institucional en materia de Ciberespacio como entorno de seguridad y desarrollo nacional.

1.3. Generar productos de Seguridad en el Ciberespacio para gestionar el Riesgo Cibernético Institucional y Marítimo Nacional.

1.4. Crear los cargos de Oficial de Seguridad de la Información para salvaguardar la infraestructura crítica institucional.

1.5. Impulsar la formación y capacitación en materia de Seguridad de la Información, Ciberseguridad y Ciberdefensa en los diferentes planteles educativos navales y aprovechar las bondades de la educación a distancia.

1.6. Adiestrar y entrenar personal en los niveles estratégico, operacional y táctico para la concepción, planeación, conducción y ejecución de las operaciones en el ciberespacio.

1.7. Obtener e implementar nuevos equipos y sistemas para fortalecer las capacidades de Seguridad en el Ciberespacio.

1.8. Impulsar la investigación y el desarrollo tecnológico para fortalecer las capacidades de Seguridad en el Ciberespacio, entendidas como Seguridad de la Información, Ciberseguridad y Ciberdefensa.

1.9. Proteger las Infraestructuras Críticas de Información propias y las correspondientes a las Instalaciones Estratégicas del País en el ámbito marítimo y portuario que se tengan a bien asignar, conforme a acuerdos de cooperación.

ACCIÓN PUNTUAL DOS

Contribuir con el esfuerzo nacional para reducir la vulnerabilidad cibernética, a través de la coordinación y cooperación con otras FF. AA., sector público, privado y académico, a favor de la Seguridad Nacional y Seguridad Interior.

2.1. Mantener y generar mecanismos de cooperación con Fuerzas Armadas y Agencias nacionales e internacionales para incrementar la capacidad de monitorear, detectar, prevenir y contrarrestar amenazas en el Ciberespacio.

2.2. Realizar acciones conjuntas con la Secretaría de la Defensa Nacional para desarrollar las capacidades de Seguridad en el Ciberespacio a través de una Estrategia de Ciberdefensa.

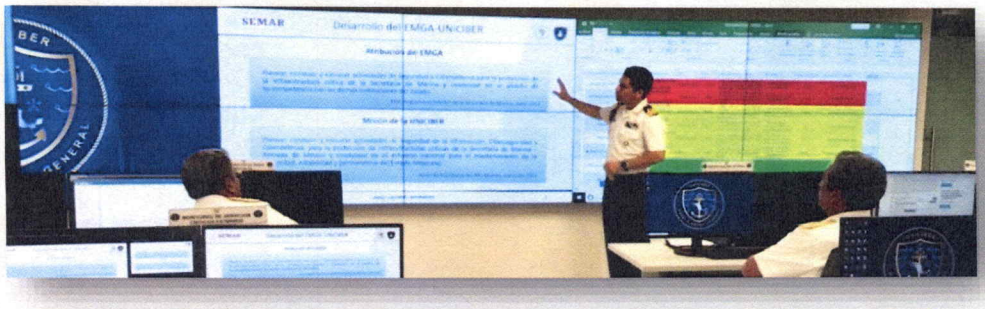
2.3. Generar mecanismos de coordinación, colaboración y cooperación con el sector público, sector privado y sector académico para coadyuvar en reducir la vulnerabilidad cibernética nacional y apoyar en la gestión del Riesgo Cibernético Marítimo Nacional.

2.4. Promover acuerdos de cooperación en reuniones de Estados Mayores, foros y comités de Ciberdefensa, Ciberseguridad y Seguridad de la Información a nivel nacional e internacional.

2.5. Participar en eventos y ejercicios de Ciberdefensa y Ciberseguridad a nivel estratégico, operacional y táctico en el ámbito nacional e internacional.

2.6. Apoyar con productos de concientización a la comunidad marítima y portuaria para mitigar las vulnerabilidades asociadas al factor humano y tecnológico.

2.7. Coordinar, colaborar y cooperar en materia de Seguridad en el Ciberespacio con las diferentes Unidades y establecimientos navales en el desarrollo de Operaciones Navales como entorno transversal al marítimo, aéreo y terrestre.



ACCIÓN PUNTUAL TRES

Planear, conducir y ejecutar actividades de seguridad de la información, ciberseguridad y ciberdefensa, a través de operaciones en el ciberespacio.

3.1. Mantener el monitoreo permanente de la infraestructura tecnológica Institucional para detectar ciberamenazas y vulnerabilidades que atentan contra los procesos críticos de la Secretaría de Marina.

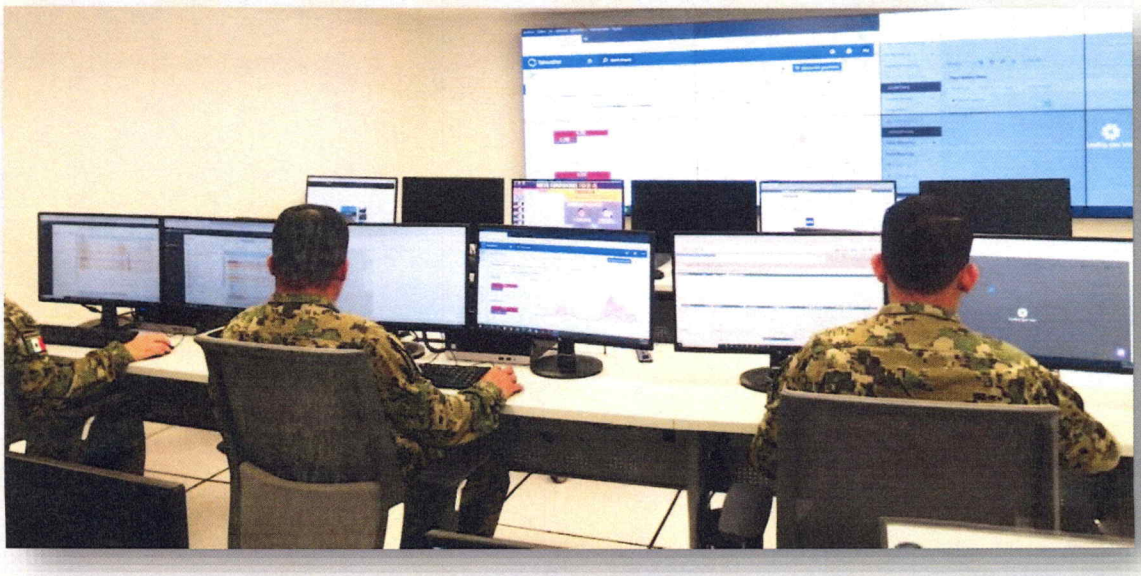
3.2. Incluir las Operaciones en el Ciberespacio dentro del Esquema General de Operaciones Navales de la Armada de México.

3.3. Formalizar el Centro de Operaciones del Ciberespacio de la Armada de México (CSIRT-MARINA y sus Equipos de Misión).

3.4. Mantener la interacción del Centro de Operaciones del Ciberespacio de la Armada de México (CSIRT-MARINA) con el Centro de Mando y Control de la Armada de México (CC2-AM) para mantener actualizado el Panorama Operacional.

3.5. Evaluar la ciberseguridad de los sistemas institucionales que soportan las Operaciones Navales y los procesos críticos institucionales.

3.6. Obtener tecnología especializada para la aplicación de cadena de custodia y el tratamiento de la evidencia digital en funciones de Autoridad Marítima Nacional.



ACCIÓN PUNTUAL CUATRO

Promover el marco jurídico, la normatividad interna y doctrina adecuada en materia de operaciones en el ciberespacio, a fin de actuar conforme a derecho en materia de ciberseguridad.

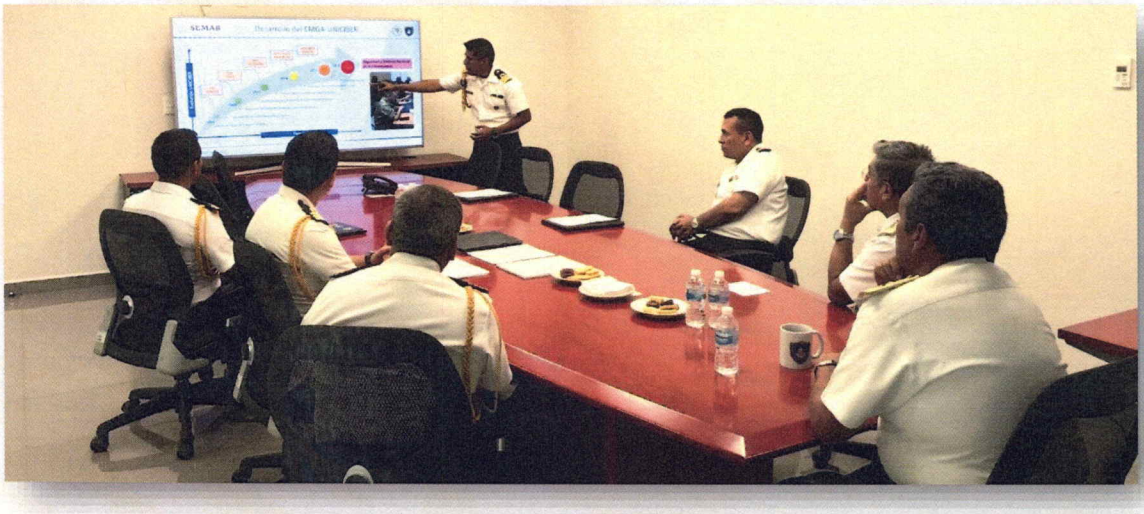
4.1. Promover las reformas legales que den sustento a la actuación de la Secretaría de Marina en el Ciberespacio.

4.2. Generar la doctrina de la Armada de México en materia de Seguridad en el Ciberespacio.

4.3. Desarrollar documentos normativos internos para prevenir eventos o incidentes de Seguridad en el Ciberespacio.

4.4. Implementar los planes y protocolos de intercambio de información, contingencia y recuperación ante eventos en materia de Ciberdefensa, Ciberseguridad y Seguridad de la Información.

4.5. Desarrollar procedimientos para la ejecución de Operaciones en el Ciberespacio.



ORGANISMOS INTERNOS COADYUVANTES

EMGA-UNICIBER en Coordinación con:	Acción Prioritaria 1	Acción Prioritaria 2	Acción Prioritaria 3	Acción Prioritaria 4
EMGA-S1	LA 1.1			
EMGA-S2		LA 2.1		LA 4.2
EMGA-S3	LA 1.4, 1.6		LA 3.2, 3.6	LA 4.2, 4.5
EMGA-S4			LA 3.3	
EMGA-S5	LA 1.7			LA 4.2
EMGA-UNICOS	LA 1.2			
EMGA-UNAJEMGA				LA 4.1, 4.2, 4.3
EMGA-UNHICUN	LA 1.2			
EMGA-UNIPLACE		LA 2.1, 2.2, 2.3, 2.4, 2.5		
CC2-AM		LA 2.7	LA 3.2, 3.4	LA 4.2, 4.4
AM-UIN	LA 1.1, 1.4, 1.9	LA 2.1, 2.5, 2.7		LA 4.2, 4.4, 4.5
AM-UNIDETEC	LA 1.7, 1.8		LA 3.5	LA 4.2
UNINAV	LA 1.2			
CESNAV	LA 1.2			LA 4.2
HENM	LA 1.2			
CENCIS	LA 1.2			
CEFCAM	LA 1.2			
AM-UNICAPAM	LA 1.2, 1.3, 1.9	LA 2.1, 2.5	LA 3.3, 3.6	
AM-UNIJUR	LA 1.4			LA 4.1
SUBRIA-DIGACOMINF	LA 1.1, 1.6		LA 3.1, 3.5, 3.6	LA 4.2, 4.4, 4.5
OFLMAY-DIGEREHUM-DIGACOPER	LA 1.1, 1.4		LA 3.3, 3.6	
OFLMAY-DIGADMON	LA 1.4, 1.7		LA 3.3, 3.6	
OFLMAY-DIGADQUIS	LA 1.4. 1.7		LA 3.6	
OFLMAY-DIGAPROP	LA 1.1, 1.4		LA 3.3	

MARINA

SECRETARÍA DE MARINA

ESTRATEGIA INSTITUCIONAL PARA EL CIBERESPACIO