MARISMA-SHIPS: Un nuevo patrón de riesgos para el entorno marítimo basado en la metodología MARISMA

Ferney MARTÍNEZ
Grupo GSyA - Grupo PRODIN
Universidad de Castilla-La Mancha - COTECMAR
Ferney.Martinez@alu.uclm.es

Luis Enrique SÁNCHEZ
Grupo de Seguridad y Auditoría – GSyA
Universidad de Castilla-La Mancha
Luise.Sanchez@uclm.es

Antonio SANTOS-OLMO
Grupo de Seguridad y Auditoría – GSyA
Universidad de Castilla-La Mancha
Antonio.Santosolmo@uclm.es

David G.ROSADO
Grupo de Seguridad y Auditoría – GSyA
Universidad de Castilla-La Mancha
David.GRosado@uclm.es

Eduardo FERNÁNDEZ-MEDINA
Grupo de Seguridad y Auditoría – GSyA
Universidad de Castilla-La Mancha
Eduardo.Fdezmedina@uclm.es

Resumen- **La ciberseguridad es crucial para prevenir, detectar y responder rápidamente a los ataques garantizando la continuidad y seguridad de las operaciones en una industria marítima cada vez más asediada. El artículo presenta una innovadora técnica de análisis de riesgos marítimos basada en una metodología de gestión de la seguridad denominada MARISMA y una herramienta en la nube llamada eMARISMA. Desarrollamos la definición del patrón MARISMA-SHIPS luego de analizar los estándares y recomendaciones para definir los elementos del patrón y alinearlos con las recomendaciones de la ENISA y el marco de trabajo de la NIST. Se presenta un caso de un buque a bordo de un astillero en el que se evidenció la adaptabilidad de MARISMA-SHIPS a cualquier elemento del ámbito marítimo. Esto resalta la capacidad de esta metodología para ser implementada con éxito en diferentes entornos, situaciones y dominios en el ámbito marítimo, demostrando su versatilidad y eficacia en la gestión de riesgos cibernéticos.**

***Index Terms*- Ciberseguridad marítima, Marisma, Análisis de riesgos**

Tipo de contribución: *Track de Investigación*

I. INTRODUCCIÓN

La industria marítima se ha posicionado como un sector de vital importancia para la economía global por su influencia en actividades comerciales, turísticas y militares, donde la exponencial aparición de las tecnologías de la información ha hecho que la ciberseguridad se convierta en un tema de amplia transcendencia [1] por sus numerosas ventajas y aportes en términos de eficiencia y operatividad.

Los buques modernos están dotados con equipos y sistemas que los exponen a diferentes vulnerabilidades haciéndolos propensos a una amplia gama de ataques cibernéticos [2-16] colocando en riesgo a tripulantes, carga, medio ambiente, operaciones, etc., que hace que los expertos en el campo de la ciberseguridad centren su mayor esfuerzo en desarrollar capacidades para la prevención [17], y fortalecimiento de la detección y respuesta a los ciberataques buscando contrarrestar las diferentes estrategias de ataque [18]. Ante el escenario descrito, donde los sistemas marítimos son tan vulnerables a ciberataques como cualquier sistema industrial donde se puede ver afectado su modelo de negocio [19], se hace necesario la implementación de políticas como la emitida por la Organización Marítima Internacional [20], que propende la generación de normas de mitigación.

Con lo anterior la implementación de un modelo o patrón, para abordar y mitigar los riesgos de manera efectiva en el entorno marítimo se vuelve una herramienta que permite garantizar la confiabilidad, integridad y disponibilidad tanto de los sistemas y datos a bordo como los que fluyen por la cadena de suministros marítimos.

Este patrón requiere ser implementado mediante una metodología de análisis que base su gestión en el uso de patrones, para lo cual la denominada "MARISMA" (Metodología para el Análisis de Riesgos en Sistemas de Información, utilizando Meta-Patrón y Adaptabilidad) que fue analizada en [21], logra reutilizar el conocimiento soportando diferentes tipos de casos minimizando el esfuerzo en los procesos y la aplicación en escenarios reales, destacando el realizado en entornos Big Data [22], o la gestión y control de riesgos en un Cyber-physical systems (CPS) con MARISMA-CPS [23].

Este artículo define un patrón de ciberseguridad marítimo al que llamaremos MARISMA-SHIPS que, basándose en la metodología de MARISMA, busca realizar una gestión y control de riesgos en un entorno marítimo. La propuesta ha tenido en cuenta los principales estándares que son analizados al largo del artículo incluyendo las recomendaciones de Gestión de Riesgos Cibernéticos para Puertos emitidas por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) [24] y el marco de trabajo desarrollado por el National Institute of Standards and Technology (NIST) [17] que permite analizar, gestionar y reducir los riesgos en el sector marítimo.

El resto del artículo se estructura de la siguiente forma: En la Sección 2 se realiza un análisis de los diferentes marcos, metodologías, estándares, etc. relacionados con la ciberseguridad marítima. En la Sección 3 se hace una descripción del entorno general y las principales fortalezas del marco de trabajo MARISMA que permite tener claridad de la definición de un patrón. En la Sección 4 se parametriza y explica el patrón MARISMA-SHIPS, para luego en la Sección 5 reflejar la aplicación y resultados en un caso de estudio en un astillero real, la Sección 6 finalmente presenta las diferentes conclusiones obtenidas y líneas de trabajo futuro.

II. MARCO NORMATIVO EN CIBERSEGURIDAD MARÍTIMA

A partir de 2017 la Organización Marítima Internacional (OMI) [1], marcó un punto de partida que posteriormente en el 2018, y con base en el marco del NIST, publicó las guías de

ciberseguridad para buques [17] con acciones y recomendaciones en ciberseguridad marítima, siendo éstas objeto de diferentes actualizaciones a lo largo del tiempo. A estas iniciativas también se ha unido la ENISA (Agencia de la Unión Europea para la Ciberseguridad) con la publicación de una guía para las buenas prácticas en puertos [24], al igual que la OCIMF (Oil Companies International Marine Forum, incluyo en sus guías el componente específico que refiere a la seguridad de los sistemas de información. De igual forma, la IMCA (International Maritime Contractors Association), también realiza actualizaciones a sus recomendaciones en ciberseguridad en su guía IMCA SEL 037/M 226 [25].

Los entes mencionados son algunos de las que ofrecen asistencia estratégica a organismos internacionales como la OEA (Organización de Estados Iberoamericanos) [2] y la OTAN (Organización del Tratado del Atlántico Norte) [26]. La Tabla I resume los aportes de las organizaciones privadas y oficiales más representativas: NIST, ISO, COBIT, BSI, OWASP [27], ENISA, CIS, SABSA, PCI DSS, Zero TRUST, ISA/IEC 62443, IEC 62351, DoD RMF (Department of Defense Risk Management Framework), CSS (Cybersecurity Standards for Ships), CMMC (Cybersecurity Maturity Model Certification), IMO Guidelines on Cyber Risk Management, y los compara en las siguientes características: (O) Orientación y ámbito de aplicación, (TP) Tipo de Propuesta en la que se aplica la carcaterística -marco de trabajo, estandar, directriz, etc.-, (HS) Identifica si cuenta con una Herramienta de Soporte informático para su aplicación, (GB) si ha sido Generado para Buques, (AM) ha sido Adaptado al Sector Marítimo, (GR) en su estructura Aplica Gestión de Riesgos, (C) cuenta con procesos que incluyen la Concienciación, (CC) presenta de manera parcial el abordaje de Cultura de Ciberseguridad.

Tabla I

No	NOMBRE	O	TP	HS	GB	AM	GR	C	CC
1	NIST	Gr	Mt	No	No	No	Sí	Sí	Sí
2	ISO27001	Gr	Est	No	No	No	Sí	Sí	Sí
3	COBIT	Em	Mt	No	No	No	Sí	Sí	Sí
4	BSI IT	Gr	Est	No	No	No	Sí	Sí	Sí
5	OWASP	Te	Lc	Sí	No	No	Sí	Sí	No
6	ENISA	Gr	Mt	No	No	No	Sí	Sí	Sí
7	CIS	Te	Lc	No	No	No	Sí	Sí	No
8	SABSA	Em	Mt	Sí	No	No	Sí	Sí	Sí
9	PCI DSS	In	Est	No	No	No	Sí	Sí	Sí
10	Zero Trust	Te	Ms	No	No	No	Sí	Sí	No
11	ISA/IEC 2443	Te	Est	No	Sí	Sí	Sí	Sí	Sí
12	IEC	Te	Est	No	Sí	Sí	Sí	Sí	Sí
13	DoD RMF	Gu	Mt	No	No	No	No	Sí	No
14	CSS	In	Est	No	Sí	Sí	Sí	Sí	Sí
15	CMMC	Gu	Mt	No	No	No	No	Sí	Sí
16	IMO	In	Dir	No	Sí	Sí	Sí	Sí	Sí

O: (Gr) General, (Em) Empresarial, (Te) Técnica, (In) Industrial, (Gu) Gubernamental,
TP: (Mt) Marco de trabajo, (Es) Estándar, (Lc) Lista de control, (Ms) Modelo de seguridad, (Di) Directrices.

III. DESCRIPCIÓN DE MARISMA

El marco de trabajo MARISMA es un desarrollo estructurado y sistemático cuyo propósito se enfoca en evaluar y mejorar mediante una metodología: La confiabilidad, disponibilidad y mantenibilidad (RAM por sus siglas en inglés Reliability, Availability, Mantenibility), de los sistemas a los que le es aplicado este framework que es adaptable a cualquier tipo de entorno [28]. MARISMA está conformado por cuatro elementos (Ver Fig. 1), siendo dos de estos bases de la metodología: Primero, la denominada meta-patrón, tiene como principal objetivo de dar soporte a los diferentes modelos de información de la metodología, y contiene los elementos necesarios para poder realizar un análisis de riesgos y su posterior gestión, el meta-patrón será una estructura común para todos los patrones. El segundo elemento se subdivide en tres procesos que buscan la generación de patrones, la generación del análisis y gestión del riesgo, y el mantenimiento dinámico del análisis de riesgos, que tienen como fin ocuparse del ciclo de vida del análisis y la gestión de todos los riesgos. Al marco de trabajo MARISMA se suma un tercer elemento con una base de conocimiento de patrones, que busca estar en constante agrupación. Y finalmente, el cuarto elemento eMARISMA que representa y soporta toda la metodología permitiendo automatizar el uso del marco de trabajo. El modelo de datos del meta-patrón se muestra en la Fig. 2 donde se identifica la capacidad que tiene el patrón de heredar los elementos comunes a cualquier proceso definido en el meta-patrón para luego ser complementados y adaptados en un contexto específico. Los detalles del modelo y un ejemplo fueron definidos en detalle en [28].

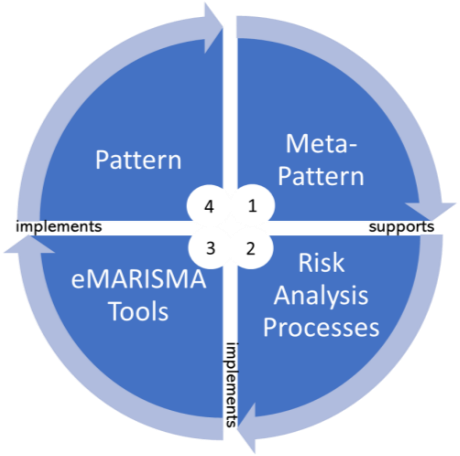

Fig. 1. Elementos de MARISMA

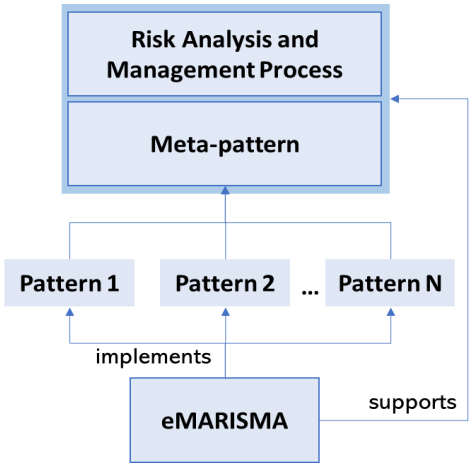

Fig. 2. Esquema general de MARISMA

Para la construcción del patrón, se realiza un proceso de revisión del estado del arte identificando los elementos normativos y operativos como estándares, guías, propuestas, etc. focalizando siempre esta búsqueda hacia el entorno marítimo. Con lo anterior se establece: dominio, controles, amenazas y dimensiones que alimentan de la información requerida al meta-patrón. Para el caso de MARISMA-SHIPS se han tenido en consideración la información suministrada por la ENISA, NIST e ISO [16], donde se detallan controles, taxonomías de activos, amenazas y dimensiones base para realizar las iteraciones para la construcción del patrón.

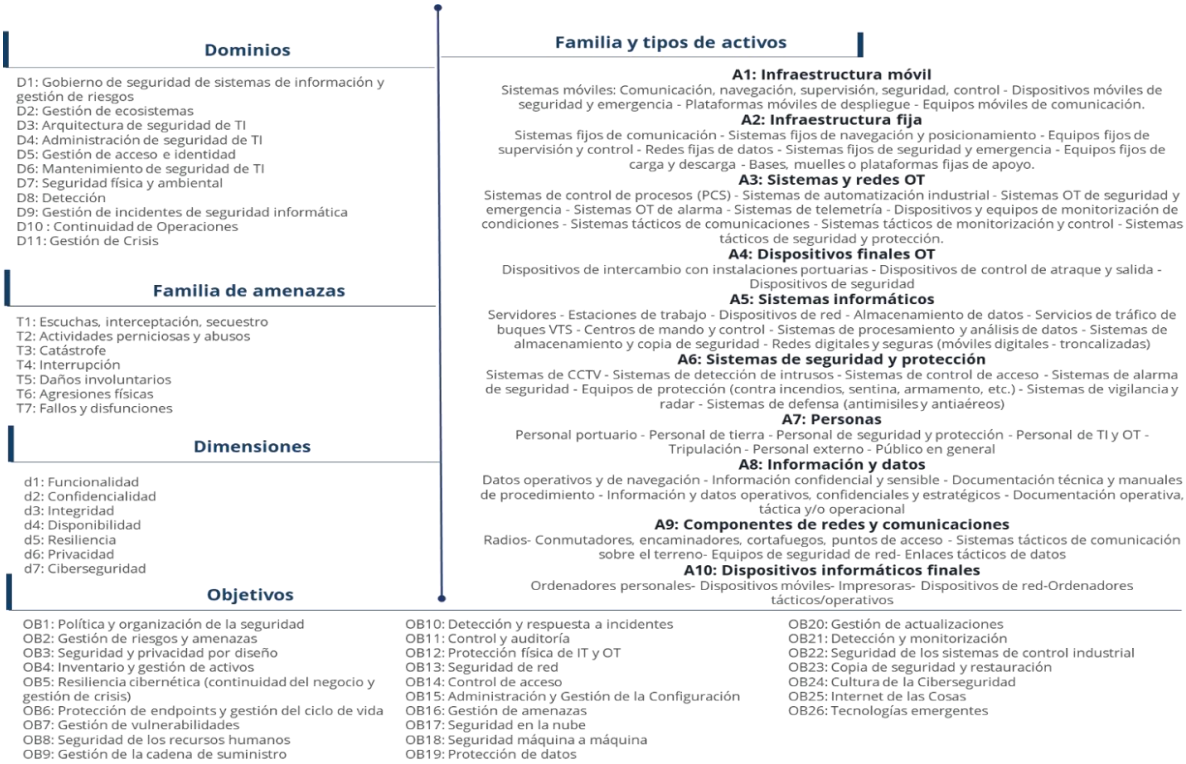

Fig. 3. Componentes de MARISMA-SHIPS

IV. DEFINICIÓN DEL PATRÓN

Para aprovechar el diseño modular del meta-patrón de MARISMA, y crear el patrón MARISMA-SHIPS se realiza una selección de todos los elementos que están involucrados en el ambiente marítimo, haciendo una clara identificación de aquellos que impactan de manera directa la ciberseguridad en cualquiera de sus componentes, los datos resultantes son comparados y analizados con los estándares, guías, etc. Los elementos que serán usados en los análisis de riesgos para el ambiente marítimo se muestran en la Fig. 3 y se desarrollan a continuación:

A. Normas y Marcos de Referencia para el sector marítimo:

El marco de trabajo del NIST es ampliamente utilizado en la ciberseguridad del sector marítimo. Aunque su enfoque principal es la industria, ha generado guías y métodos reconocidos en este ámbito, específicamente orientados a proteger los sistemas y activos digitales en operaciones marítimas, especialmente en buques.

El Marco de Ciberseguridad NIST-CSF, utilizado en diversos entornos, incluido el ámbito marítimo, establece un enfoque sistemático y coherente para abordar los desafíos de ciberseguridad en el sector marítimo. La identificación y gestión de riesgos, junto con la protección de los activos críticos, facilitan la adaptabilidad, escalabilidad e integración de tecnologías, así como la implementación de buenas prácticas. Estas fortalezas son fundamentales para ser incorporadas en MARISMA-SHIPS.

La normativa de seguridad de redes y sistemas de la Unión Europea desempeña un papel significativo dentro del contexto de MARISMA, al establecer criterios mínimos que son tenidos en cuenta por la ENISA y que están dirigidos a garantizar la integridad, confidencialidad y disponibilidad de la información y la infraestructura digital.

Asimismo, el informe "Directrices para la Ciberseguridad en el Sector Marítimo", emitido por la ENISA, proporciona una detallada información sobre recomendaciones, pautas y directrices para fortalecer la ciberseguridad en el ámbito marítimo. En dicho documento se tratan aspectos cruciales para MARISMA-SHIPS, como la evaluación de riesgos, la gestión de incidentes y la capacidad de respuesta ante ataques, así como mecanismos de concienciación y formación. Además, se destaca la importancia de la cooperación y coordinación entre los diversos actores del sector naval, subrayando su vitalidad para una defensa conjunta. La identificación de las amenazas cibernéticas para el sector marítimo es el resultado del análisis de la taxonomía de amenazas que se proponen por [28-29] con un clasificación y detalle de aquellas de mayor relevancia, de igual manera se genera un listado de activos críticos que fue analizados por parte del grupo de investigadores, mediante la realización de mesas de trabajo con un universo de 17 individuos de diferentes temáticas marítimas: personal de astillero, tripulación del buque, personal de TIC´s, seguridad informática y personal técnico de a bordo, que mediante el desarrollo de una metodología colaborativa, seleccionaron la línea de activos de mayor importancia en el entorno marítimo, los resultados de la selección fueron aplicados en el patrón MARISMA-SHIPS.

B. Componentes del patrón MARISMA-SHIPS

Dominios, objetivos y controles

El comité de expertos colaboradores del proyecto, ha tomado como punto de partida la información contenida las recomendaciones de la ENISA [30] para que sumado a su experticia, consolidaran las áreas o principales categorías para abarcar los diferentes aspectos de la seguridad cibernética, estos dominios seleccionados permiten establecer una estructura base de organización y abordaje de los diferentes aspectos de ciberseguridad a su vez que clasifican los controles agrupadas en dominios específicos, con ello los usuarios de

eMARISMA pueden identificar que controles son los más apropiados para proteger los activos identificados contra las amenazas reconocidas reduciendo riesgos potenciales. Los dominios y familia de amenazas se muestran en la Fig. 3 .

Tipos de activos

El informe de Gestión de Riesgos Cibernéticos para Puertos de la ENISA [31] y la metodología SP800 enfocada en la seguridad de los sistemas de información y redes del NIST brinda una clasificación de familias y tipos de activos que son sugeridos para manejar la seguridad de la información y la gestión de riesgos en el ambiente marítimo. La Fig. 3 muestra los diferentes tipos de activos que deben tenerse en cuenta en el patrón de ciberseguridad para el sector marítimo MARISMA-SHIPS identificando la clasificación por familias y tipos que debemos incorporar en la propuesta

Familia de Amenazas y tipos de amenazas

Para establecer las familias y tipos de amenazas que deben ser incorporadas a MARISMA-SHIPS se analizaron las taxonomías propuestas por ENISA y NIST, la clasificación final se ve en la Fig. 3 y el detalle de los tipos en la tabla II.

Tabla II:
AMENAZAS Y TIPOS PARA MARISMA-SHIPS

Familia de Amenazas	Resumen tipos de amenazas
Escuchas, interceptación, secuestro	Secuestro de protocolos de comunicación, reconocimiento de red, fuga de información, reproducción de mensajes, pruebas de penetración, administración errónea, etc.
Actividad nefasta y abuso	Kits de explotación, ataques dirigidos, Denegación de Servicio, ataques a la privacidad, modificación de señales, spoofing / jamming, etc.
Desastre Interrupciones	Naturales, ambientales, tecnológicos. Fallas de los dispositivos, sistemas, pérdida de servicios de apoyo, ausencia de personal, etc.
Daño no intencional	Fuga de datos/información confidencial, interceptaciones, manipulaciones
Agresiones físicas	Modificación o destrucción de dispositivos, accesos no autorizados, terrorismo, hacktivismo, coacción, extorsión, etc. o corrupción
Fallos y mal funcionamiento	Fallas de sistemas vitales – no vitales, de terceros, interrupción de servicios, etc.

Dimensiones

La Fig. 3 consolida las dimensiones para ser usadas en MARISMA-SHIPS y son resultado del proceso de aporte y análisis por parte de los expertos, estas dimensiones propuestas son fundamentales para diseñar e implementar el patrón de ciberseguridad y se describen en detalle en la tabla III.

Matriz objetivo-dominio-amenazas

En base al informe de ENISA [31] y las actualizaciones del NIST se definen los objetivos de control basado en el conjunto de controles (Ver Tabla V) y se les asigna a un dominio, el resultado final se observa en la Tabla VI, por ejemplo (subrayado en la Tabla VI) el objetivo "Política y organización de la seguridad" se ha relacionado con una serie de controles clasificados dentro de los dominios: D1: Gobierno de seguridad de sistemas de información y gestión de riesgos, D9: Gestión de incidentes de seguridad informática, D10 : Continuidad de Operaciones y D11: Gestión de Crisis, y para cada uno de estos dominios se identifica el control relacionado con ese objetivo.

La definición del patrón MARISMA-SHIPS introduce un enfoque integral para la gestión de riesgos y la protección de la información. Este enfoque se ha estructurado con un marco de referencia que establece estándares y procedimientos, así como la identificación y análisis de riesgos específicos en el ámbito marítimo. Además, incluye requisitos de seguridad que garantizan la protección de activos, ya sean civiles o militares, junto con la implementación de controles adecuados y un proceso de seguimiento con mejora continua. Estos elementos están interrelacionados de manera coherente y secuencial, creando un enfoque holístico y proactivo para mitigar los riesgos cibernéticos. La Sección V del documento presenta los resultados obtenidos en la herramienta eMARISMA mediante la aplicación de MARISMA-SHIPS en una unidad marítima.

V. ESTUDIO DE CASO: BUQUE DUAL

En el caso de estudio que se presenta, se aplicó la propuesta de MARISMA-SHIPS a un buque de propósito dual, una embarcación diseñada y construida para llevar a cabo diversas funciones o tareas en diferentes escenarios, ya sean civiles o militares. Esta versatilidad expone los sistemas y equipos a una variedad de riesgos y amenazas cibernéticas durante su uso operacional. Las actividades correspondientes al caso de estudio se llevaron a cabo en las instalaciones de la Corporación para el Desarrollo de la Industria Naval Marítima y Fluvial (COTECMAR) en Cartagena, Colombia, en América del Sur.

A. Definición de dimensiones, activos

En la etapa inicial del análisis del riesgo con MARISMA-SHIPS se definieron un conjunto de dimensiones que se muestran en la Fig. 3 y se explican en la tabla III.

Tabla III:
DIMENSIONES PROPUESTAS PARA MARISMA-SHIPS

Dimensión	Descripción
1. Funcionalidad:	Capacidad de los sistemas y componentes de seguridad para realizar sus funciones previstas de manera efectiva.
2. Confidencialidad:	Busca la protección de la información sensible contra el acceso no autorizado.
3. Integridad:	Refiere a la protección de la información contra modificaciones no autorizadas o no deseadas.
4. Disponibilidad:	Garantiza que los sistemas y componentes de seguridad estén disponibles y sean accesibles cuando se necesiten.
5. Resiliencia:	Se refiere a la capacidad para resistir, adaptarse y recuperarse de amenazas y ataques cibernéticos.
6. Privacidad:	Su eje es la protección de la información personal y sensible de los individuos.
7. Ciberseguridad	Elementos que garantizan la seguridad de los sistemas frente a amenazas digitales.

B. Definición de activos para el caso de estudio

La selección de activos para ser incorporados en el análisis con la metodología MARISMA implico una cuidadosa evaluación de los sistemas críticos a bordo del buque (navegación, comunicaciones, propulsión, administrativos, entretenimiento, etc.). Esta selección inició con un mapeo entre la base de MARISMA-SHIPS y los activos utilizados en las operaciones marítimas. Posteriormente se establece una clasificación basada en la importancia del activo para las operaciones y seguridad del buque. Una vez se tiene la consolidación y clasificación que se presenta en la Fig. 3 se incorpora esta información a la herramienta web eMARISMA.

C. *Definición de amenazas para el caso de estudio*

El proceso continua con la identificación de las amenazas que pueden ejercer algún nivel de afectación a los sistemas del buque, para esto se toman las amenazas del patrón MARISMA-SHIPS y se identifican aquellas que pueden afectar directamente el buque para indicar los porcentajes de degradación del valor del activo (daño causado) y de la probabilidad de ocurrencia de un ataque, dicho valor debe ser seleccionado entre 0 y 100. Un ejemplo se puede ver (subrayado) en la Tabla IV donde la amenaza: Ataque por denegación de servicio es del tipo de amenaza: Ataque dirigido y pertenece a la familia de amenazas: Actividad nefasta y abuso.

D. *Análisis del riesgo para el caso de estudio*

Una vez completadas las etapas anteriores, se debe proceder con el análisis del impacto de las amenazas en cada uno de los activos del buque, de acuerdo con las dimensiones seleccionadas. Esto permite calcular la degradación del activo cuando la amenaza afecta al buque. Los valores por defecto son asignados teniendo como base los porcentajes de degradación establecida ya sea por: a) Los valores asignados en el paso anterior, b) Los predeterminados por la herramienta en función de su conocimiento o c) Los que puedan ingresarse manualmente a concepto del grupo de expertos, cualquiera que sea la mecánica seleccionada, la herramienta eMARISMA por su versatilidad permite hacer estas valoraciones por asignación o por modificación directa del valor.

E. *Análisis de riesgos: resultados*

Para concluir el proceso de análisis, la utilización de una lista de control de seguridad permite llevar a cabo una verificación interna que proporciona un nivel real de seguridad del sistema. Esta verificación usa los dominios, objetivos de control y controles usados en las divisiones de las listas de checklist de eMARISMA. Con lo anterior se identifica la cobertura de seguridad actual con los controles que ya están implementados y cuáles son los que deben ser aplicar o descartar, determinando con ello el nivel de seguridad actual. La lista brinda una visión general de debilidades y fortalezas base para la toma de decisiones. La Fig. 4 muestra el contexto general del tablero con la información de cobertura en todos los niveles de dominios, objetivos y controles que permite su seguimiento de manera gráfica. Los diagramas de Kiviat presentes en eMARISMA son otra herramienta versátil para visualizar y comparar datos multidimensionales, por ejemplo: por dominios (Fig. 5) donde se identifica el nivel de cumplimiento del dominio IAM (Gestión de acceso e identidad) en 50%. En la categoría por objetivos de control (Fig. 6) se ve como el CMS-TP-06 que corresponde Restringir cuentas genéricas (ver Tabla V) se califica con 100%.

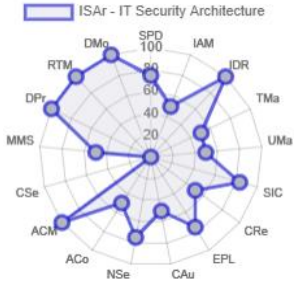

Fig. 5: Diagramas de Kiviat categoría dominios generados

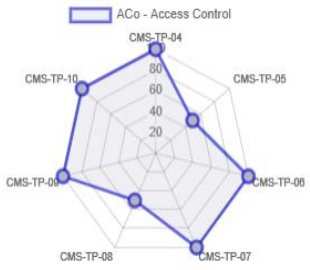

Fig. 6: Diagramas de Kiviat categoría objetivos de control

Fig. 4: Ejemplo de las listas de control del tablero de eMARISMA

Del mismo modo, eMARISMA cuenta con una variedad de herramientas visuales y de texto, tales como mapas de calor y mapas de riesgos, entre otras opciones, las cuales suministran al experto información detallada en tiempo real con el fin de facilitar la toma de decisiones.

Tabla IV:
AMENAZAS PARA CASO DE ESTUDIO MARISMA-SHIPS

Familia de Amenazas	Tipo de Amenazas	Amenazas para el caso de estudio
Escuchas, interceptación, secuestro	Secuestro de protocolo de comunicación, Reconocimiento de red, Interceptación o fuga de información, Secuestro de sesión, Recopilación de información, Reproducción de mensajes, Pruebas de penetración.	Secuestro de redes Alteración de dispositivos
Actividad nefasta y abuso	Malware, Kits de explotación, *Ataques dirigidos*, Ataque de denegación de servicios, Falsificación por dispositivos maliciosos, Ataques a la privacidad, Modificación de la información, Señales de geolocalización.	*Ataque por Denegación de Servicio a servidores operacionales*. Ingeniería social Phishing Malware
Desastre	Desastres naturales, ambientales y tecnológicos.	Daños por: Huracán Incendios
Interrupciones	Fallas de los dispositivos, Falla del sistema, Pérdida de servicios de apoyo, Caída de la red, Ausencia de personal.	Fallo en cuarto de servidores Ataque a propulsores
Daño no intencional	Sabotajes: Fuga de información confidencial, manipulaciones, etc.	Errores de configuración - malas prácticas
Agresiones físicas	Modificación destrucción de dispositivos, Accesos no autorizados, Terrorismo, Hacktivismo, Piratería, extorsión o corrupción.	Ataque informático y Ataque físico por piratas
Fallos y mal funcionamiento	Fallas de sistemas vitales, no vitales, Fallas de terceros, Interrupción de servicios.	Falla en la mesa de cartas y GPS

Tabla V:
CONSOLIDADO DE CONTROLES DE SEGURIDAD PARA EL ENTORNO MARÍTIMO POR ENISA

Controles Enfocados A Las Políticas		
Política y organización de la seguridad	PS-01	Política de Seguridad del Sistema de Información (ISSP)
	PS-02	Gobernanza de la seguridad
	PS-03	Compartir ISSP con todas las partes
	PS-04	Revisar ISSP anualmente
	PS-05	Enfoque basado en riesgos

Gestión de riesgos y amenazas	PS-06	Realizar y actualizar análisis de riesgos
	PS-07	Indicadores de seguridad y métodos de evaluación
	PS-08	Proceso de inteligencia de amenazas
Seguridad y privacidad por diseño	PS-09	Metodología de proyecto incluyendo seguridad
	PS-10	Privacidad y cumplimiento
	PS-11	Clasificación de datos
Inventario y gestión de activos	PS-12	Inventario y gestión de activos
	PS-13	Política para dispositivos y software
	PS-14	Monitoreo de activos
Resiliencia cibernética (continuidad del negocio y gestión de crisis)	PS-15	Definir objetivos y lineamientos estratégicos (BCP y DRP).
	PS-16	Parámetros de continuidad del negocio (RTO, RPO, MTO, etc.)
	PS-17	Gestión de crisis
	PS-18	Entrenamiento/ejercicios para procedimientos de recuperación
Controles Organizativos		
Protección de endpoints y gestión del ciclo de vida	OP-01	Estrategia de protección de puntos finales
	OP-02	Lista blanca de dispositivos y software
	OP-03	Gestión de cambios
	OP-04	Devolución y eliminación de dispositivos finales
Gestión de vulnerabilidades	OP-05	Proceso de gestión de vulnerabilidades
	OP-06	Procesos de inteligencia
	OP-07	Colaboración de los departamentos OT y TI
Seguridad de los recursos humanos	OP-08	Referencias profesionales del personal
	OP-09	Capacitación en Ciberseguridad
	OP-10	Programa de sensibilización
Gestión de la cadena de suministro	OP-11	Control de acceso de terceros
	OP-12	Asociación con terceros
Detección y respuesta a incidentes	OP-13	Definir categorías de incidentes
	OP-14	Política y procedimientos para la detección y respuesta de incidentes
	OP-15	Mejorar y actualizar procedimientos
	OP-16	Centro de Operaciones de Seguridad
	OP-17	Procedimientos de alerta y plan de comunicación
	OP-18	Reporte de incidentes y mejora continua
Control y auditoría	OP-19	Auditorías de ciberseguridad
	OP-20	Revisiones periódicas
Protección física de IT y OT	OP-21	Protección física para la seguridad
	OP-22	Trazabilidad de operaciones/mantenimiento
Cultura de la Ciberseguridad	OP-23	Promoción e Implementación de políticas y procedimientos.
Internet de las Cosas	OP-24	Programa integrado de seguridad de IoT
Tecnologías emergentes: IA	OP-25	Protección y control de Tecnologías Emergentes
Controles Técnicos		
Seguridad de red	TP-01	Segmentación de red
	TP-02	Escaneos de red regulares
	TP-03	Seguridad perimetral
Control de acceso	TP-04	Herramientas centralizadas para IAM
	TP-05	Estrategia de gestión de identidades
	TP-06	Restringir cuentas genéricas
	TP-07	Políticas/reglas de complejidad de contraseña
	TP-08	Autenticación multifactor
	TP-09	Control de acceso físico/remoto
	TP-10	Cuentas y revisiones de derechos de acceso
Administración y Gestión de la Configuración	TP-11	Política de instalación y configuración
	TP-12	Cuentas de administradores
	TP-13	Gestión de cuenta de privilegios
	TP-14	Redes de administración dedicadas
Gestión de amenazas	TP-15	Antimalware, antispam y antivirus
Seguridad en la nube	TP-16	Evaluación de la seguridad en la nube
	TP-17	Seguridad/disponibilidad en la nube
	TP-18	Opciones de nube para detección/respuesta
Seguridad máquina a	TP-19	Intercambios M2M seguros
	TP-20	Protocolos de comunicación segura
Protección de datos	TP-21	Criptografía
	TP-22	Anonimizar / asegurar datos personales
Gestión de actualizaciones	TP-23	Definir actualización proceso de gestión
	TP-24	Autenticidad de software/firmware
	TP-25	Verificar la fuente de actualizaciones
Detección y monitorización	TP-26	Disponibilidad de los sistemas portuarios
	TP-27	Sistema de registro
	TP-28	Sistemas de correlación y análisis de logs
Seguridad de los sistemas de control industrial	TP-29	Sistemas OT en medidas de seguridad
	TP-30	Segmentación de red entre TI/OT
	TP-31	Medidas de seguridad específicas para IoT
Copia de seguridad y restauración	TP-32	Configure copias de seguridad, mantenga y pruebe regularmente

VI. CONCLUSIONES

La investigación llevada a cabo mediante la metodología MARISMA, permitió desarrollar un patrón dirigido al ámbito marítimo al que denominamos MARISMA-SHIPS. Este patrón se ha fundamentado en estándares internacionales y en recomendaciones de expertos del sector marítimo, para su validación se ha hecho uso de la herramienta eMARISMA.

El estudio de caso expuesto en el documento se integra dentro del marco del proceso de adopción de una nueva competencia en el análisis de riesgos cibernéticos específicamente para la industria naval latinoamericana. Esto se lleva a cabo a través de COTECMAR, con el respaldo académico de la Universidad de Castilla-La Mancha y empleando una unidad marítima de tipo buque dual como caso práctico real donde se incorporan equipos de navegación y comunicaciones, sistemas de propulsión, administrativo, seguridad y defensa, CCTV, etc. Esto ha posibilitado la validación de la interacción del patrón MARISMA-SHIPS en un entorno marítimo real, enfrentando escenarios de riesgo potencial. Los resultados obtenidos han determinado que la propuesta de MARISMA-SHIPS es viable para su integración en la línea de servicios del astillero.

Se ha generado una experiencia enriquecedora por parte del grupo de investigación, que además de cerrar la brecha de trabajo entre la academia y la industria, permite enriquecer la experiencia de los investigadores para desarrollar patrones con mayor nivel de especificación, lo que conlleva a niveles análisis de riesgos más precisos.

La investigación llevada a cabo en este estudio posee una relevancia significativa para los astilleros, especialmente para COTECMAR. Esto se debe a que proporciona una base sólida para el desarrollo e implementación de estrategias de ciberseguridad que, como MARISMA, permiten evaluar los sistemas de los buques que construye y comercializa brindando un plus a sus potenciales clientes. Entre las ventajas destacadas, se encuentra la mejora en la capacidad de identificación de amenazas y vulnerabilidades específicas, lo que permite, con el uso de MARISMA-SHIPS y eMARISMA, contar con medidas proactivas para proteger los activos y salvaguardar el cumplimiento de las operaciones marítimas.

Se proyecta como línea de trabajo futuro, la generación de nuevos casos con foco a elementos propios del sector marítimo como las instalaciones portuarias, buques de investigación marítima, buques militares, etc. que permitan afinar el diseño de MARISMA-SHIPS y la explotación a cabalidad de

eMARISMA como herramienta de uso del patrón.

AGRADECIMIENTOS

Este trabajo ha sido desarrollado con financiación de los proyectos Di4SPDS (CHIST-ERA grant - PCI2023145980-2) financiado por MCIN/AEI/10.13039/501100011033 y cofinanciado por la Unión Europea, AETHER-UCLM (PID2020-112540RB-C42) financiado por MCIN/AEI/10.13039 /501100011033; ALBA-UCLM (TED2021-130355B-C31) financiado por MCIN/AEI/10.13039/501100011033/ Unión Europea NextGenerationEU/PRTR; y MESIAS (2022-GRIN-34202) financiado por FEDER. Así como por la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial, COTECMAR. Finalmente, agradecer al personal de la Armada Nacional de Colombia que participó en este trabajo, por su disposición y compromiso.

REFERENCIAS

[1] International Maritime Organization - IMO, "Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems," Web site IMO, Reino Unido, Jun. 16, 2017. Accessed: Feb. 27, 2024. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

[2] OEA, "Organización de Estados Americanos - OEA :: Quiénes Somos," Institucional - Quienes Somos. Accessed: Mar. 12, 2024. [Online]. Available: https://www.oas.org/es/acerca/quienes_somos.asp

[3] C. Mascareñas and A. I. Vázquez, "Notes on maritime cybersecurity in ship design," RINA, Royal Institution of Naval Architects - International Conference on Marine Design 2020, Papers, pp. 91–99, 2020, Accessed: Mar. 24, 2024. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85083897431&origin=resultslist&sort=plf-f&src=s&st1=Notes+on+maritime+cybersecurity+in+ship+design&sid=abf1636ee1a0cfe0a796e5151053fd79&sot=b&sdt=b&sl=61&s=TITLE-ABS-KEY%28Notes+on+maritime+cybersecurity+in+ship+design%29&relpos=0&citeCnt=0&searchTerm=

[4] D. Heering, "Ensuring cybersecurity in shipping: Reference to Estonian shipowners," TransNav, vol. 14, no. 2, pp. 271–278, Jun. 2020, doi: 10.12716/1001.14.02.01.

[5] V. Greiman, "Navigating the cyber sea: Dangerous atolls ahead," 14th International Conference on Cyber Warfare and Security, ICCWS 2019, pp. 87–93, 2019.

[6] "2021 World Automation Congress, WAC 2021," World Automation Congress Proceedings, vol. 2021-August, Aug. 2021.

[7] OMI, "International Maritime Organization." Accessed: Mar. 21, 2024. [Online]. Available: https://www.imo.org/es/About/Paginas/Default.aspx

[8] International Maritime Organization - IMO, "Guidelines on Maritime Cyber Risk Management," Web site IMO- MSC-FAL.1/Circ.3, no. Circular 3, Jul. 2017, Accessed: Feb. 27, 2022. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

[9] B. Xing, J. Dai, and S. Liu, "Enforcement of opacity security properties for ship information system," International Journal of Naval Architecture and Ocean Engineering, vol. 8, no. 5, pp. 423–433, Sep. 2016, doi: 10.1016/J.IJNAOE.2016.05.012.

[10] International Maritime Organization, "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS." Accessed: Mar. 11, 2024. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

[11] OCIMF - Oil Companies International Marine Forum, "Tanker Management and Self Assessment 3 - A Best Practice Guide." Accessed: Mar. 17, 2024. [Online]. Available: https://www.ocimf.org/es/publicaciones-y-promoci%C3%B3n/publicaciones/libros/tanker-management-and-self-assessment-3

[12] IMCA, "International Maritime Contractors Association." Accessed: Mar. 10, 2024. [Online]. Available: https://www.imca-int.com/about-imca/

[13] R. Talas, "Port security," Advanced Sciences and Technologies for Security Applications, pp. 161–172, 2020, doi: 10.1007/978-3-030-34630-0_10.

[14] Ž. Turk, B. García de Soto, B. R. K. Mantha, A. Maciel, and A. Georgescu, "A systemic framework for addressing cybersecurity in construction," Autom Constr, vol. 133, p. 103988, Jan. 2022, doi: 10.1016/J.AUTCON.2021.103988.

[15] IEC, "Normalización española IEC 61162-460:2018 ." Accessed: Mar. 11, 2023. [Online]. Available: https://www.une.org/encuentra-tu-norma/busca-tu-norma/iec?c=63097

[16] International Organization for Standardization, "ISO - ISO 16425:201." Available: https://www.iso.org/standard/56739.html

[17] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology".

[18] R. Safi and G. J. Browne, "Detecting Cybersecurity Threats: The Role of the Recency and Risk Compensating Effects," Information Systems Frontiers, vol. 25, no. 3, pp. 1277–1292, Jun. 2023, doi: 10.1007/S10796-022-10274-5.

[19] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," Comput Ind, vol. 103, pp. 97–110, Dec. 2018, doi: 10.1016/J.COMPIND.2018.09.004.

[20] OMI, "GUIDELINES ON MARITIME CYBER RISK MANAGEMENT," MSC-FAL 1-Circ 3.docx.

[21] L. Enrique Sánchez, A. Santos-Olmo Parra, D. G. Rosado, and M. Piattini, "Managing Security and its Maturity in Small and Medium-sized Enterprises," JUCS - Journal of Universal Computer Science 15(15): 3038-3058, vol. 15, no. 15, pp. 3038–3058, 2009, doi: 10.3217/JUCS-015-15-3038.

[22] D. G. Rosado, J. Moreno, L. E. Sánchez, A. Santos-Olmo, M. A. Serrano, and E. Fernández-Medina, "MARISMA-BiDa pattern: Integrated risk analysis for big data," Comput Secur, vol. 102, p. 102155, Mar. 2021, doi: 10.1016/J.COSE.2020.102155.

[23] D. G. Rosado et al., "Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern," Comput Ind, vol. 142, p. 103715, Nov. 2022, doi: 10.1016/J.COMPIND.2022.103715.

[24] Agencia de la Unión Europea para la Ciberseguridad - ENISA, "Agencia de la Unión Europea para la Ciberseguridad - ENISA." Accessed: Mar. 27, 2023. [Online]. Available: https://www.enisa.europa.eu/

[25] IMCA, "Security measures and emergency response guidelines – IMCA." Accessed: Mar. 13, 2023. [Online]. Available: https://www.imca-int.com/product/security-measures-and-emergency-response-guidelines/

[26] Organización del Tratado del Atlántico Norte – OTAN, "OTAN - UNA ALIANZA POLÍTICA Y MILITAR," 2.1 Una alianza Política y MIlitar. Accessed: Mar. 12, 2023. [Online]. Available: https://www.nato.int/nato-welcome/index_es.html

[27] "OWASP Foundation, the Open-Source Foundation for Application Security | OWASP Foundation." Accessed: Mar. 27, 2023. [Online]. Available: https://owasp.org/

[28] A. Santos-Olmo, L. E. Sánchez, D. G. Rosado, E. Fernández-Medina, and M. Piattini, "Applying the Action-Research Method to Develop a Methodology to Reduce the Installation and Maintenance Times of Information Security Management Systems," Future Internet 2016, Vol. 8, Page 36, vol. 8, no. 3, p. 36, Jul. 2016, doi: 10.3390/FI8030036.

[29] ENISA, "Taxonomía de amenazas ." Accessed: Jul. 26, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[30] P. O. of the E. Union, "Baseline security recommendations for IoT in the context of critical information infrastructures.," Dec. 2017, doi: 10.2824/03228.

[31] ENISA, "Guidelines - Cyber Risk Management for Ports — ENISA." Accessed: Jul. 26, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

Tabla VI:
CLASIFICACIÓN DE OBJETIVOS DE CONTROL ASIGNADOS POR DOMINIO

	DOMINIOS										
OBJETIVOS	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11
Política y organización de la seguridad	PS-01, 02,03,04	-	-	-	-	-	-	-	PS-01,03	PS-02,03,04	PS-02,03,04
Gestión de riesgos y amenazas	PS-05		PS-07			PS-06,08	PS-09	PS-07,08	PS-05,07	PS-05	
Seguridad y privacidad por diseño	PS-09		PS-09,11	PS-09			PS-09		PS-10,11	PS-10	
Inventario y gestión de activos			PS-12,14		PS-13	PS-12	PS-13				
Resiliencia cibernética (continuidad del negocio y gestión de crisis)	PS-15		PS-16	PS-16				PS-15	PS-16,17,18	PS-15	PS-15,16,17
Protección de endpoints y gestión del ciclo de vida			OP-01,03	OP-01, 04	OP-02	OP-01,02					
Gestión de vulnerabilidades	OP-07	OP-05, 06								OP-06, 07	
Seguridad de los recursos humanos	OP-09,10			OP-08			OP-09,10		OP-10		
Gestión de la cadena de suministro		OP-11,12			OP-11,12						
Detección y respuesta a incidentes	OP-14	OP-16	OP-16	OP-16				OP-13,14,16	OP-15,16, 17,18	OP-15	OP-14,16, 17,18
Control y auditoría		OP-19	OP-20	OP-19,20	OP-19	OP-19		OP-19	OP-20		
Protección física de IT y OT				OP-21,22	OP-22	OP-22	OP-21				
Seguridad de red		TP-02	TP-01,03	TP-01,02	TP-02	TP-02	TP-03	TP-03			
Control de acceso		TP-06,08	TP-04,08	TP-08	TP-04,05,06, 07,08,09,10		TP-04				
Administración y Gestión de la Configuración			TP-11	TP-11,13	TP-12,13	TP-13				TP-11	TP-11
Gestión de amenazas			TP-15	TP-15		TP-15					
Seguridad en la nube		TP-16,17	TP-17	TP-16,17					TP-18	TP-18	TP-18
Seguridad máquina a máquina			TP-20	TP-19		TP-19,20		TP-20			
Protección de datos			TP-21	TP-21		TP-22		TP-21			
Gestión de actualizaciones	TP-23		TP-23,25	TP-23,24,25	TP-23						
Detección y monitorización			TP-27	TP-28	TP-27	TP-26		TP-26,28		TP-28	
Seguridad de los sistemas de control industrial		TP-30	TP-29, 30,31	TP-29,30,31	TP-29,31	TP-31	TP-29		TP-29	TP-29	
Copia de seguridad y restauración				TP-32					TP-32	TP-32	TP-32
Cultura de la Ciberseguridad	OP-23		OP-23			OP-23			OP-23		OP-23
Internet de las Cosas		OP-24	OP-24					OP-24	OP-24	OP-24	
Tecnologías emergentes: IA	OP-25		OP-25					OP-25	OP-24	OP-25	

Dominios:
D1: Gobierno de seguridad de sistemas de información y gestión de riesgos
D2: Gestión de ecosistemas
D3: Arquitectura de seguridad de TI
D4: Administración de seguridad de TI
D5: Gestión de acceso e identidad
D6: Mantenimiento de seguridad de TI
D7: Seguridad física y ambiental
D8: Detección
D9: Gestión de incidentes de seguridad informática
D10 : Continuidad de Operaciones
D11: Gestión de Crisis