Diseño de un sistema de ciberseguridad aplicable a un buque de la Armada

Autor: Carrasco Sandino, Miguel

Director/es: Rodelgo Lacruz, Miguel.

Contacto: mcarsan@fn.mde.es mrodelgo@cud.uvigo.es

Resumen: El presente trabajo tiene como objetivo sentar las bases del diseño de un sistema de ciberdefensa que se pueda instalar en buques de la Armada Española. La creciente adopción de soluciones tecnológicas de automatización en dichos buques, hace que se vean más expuestos a ciber ataques con los consecuentes riesgos asociados. Por lo tanto, en el presente texto, se pretende establecer una metodología adecuada para el desarrollo del sistema, identificar los requisitos aplicables a un sistema de ciberdefensa, caracterizar los sistemas a bordo que deben ser supervisados, y realizar un análisis de riesgos de dicha caracterización.

Todos estos pasos se han llevado a cabo sin perder de vista que las instalaciones a bordo de los buques poseen cierto grado de clasificación en función de la información que manejen, y por lo tanto, es de aplicación cierta normativa que no se puede obviar en el diseño de un sistema que supervise todos los sistemas conectados a bordo.

Por último, se ofrece una configuración tanto de software como de hardware que sea capaz de soportar la instalación y operación del sistema de ciberdefensa, así como el procedimiento de desarrollo del software necesario hasta llegar a una solución de compromiso que cubra la totalidad de los requisitos del sistema, identificados al principio del proceso. Adicionalmente se incluye una planificación tentativa de la duración de los diferentes procesos.

Palabras clave: Ciberdefensa, sistema, buque, requisitos, desarrollo, análisis.

---

1. Introducción

La adopción de la tecnología de automatización en las plataformas de la Armada es un hecho patente. La desaparición del servicio militar obligatorio a principios del siglo XXI, forzó la adopción de dotaciones más reducidas en los buques, desarrollando nuevas tecnologías que permitían el pilotaje

de la maquinaria a distancia, y de manera desatendida. Todas estas tecnologías, sumadas a las cada vez más complejas propias de un buque de guerra moderno, como son los sensores, sistema de combate y comunicaciones, actualmente están basadas en redes informáticas. Los buques de guerra poseen kilómetros de redes en su interior, que conectan los diferentes elementos.

Por lo tanto, el riesgo de ciber ataques lleva presente desde el mismo momento en que se adoptaron dichas tecnologías. Esta realidad ha forzado a las FAS a desarrollar soluciones de ciberdefensa para que sean instaladas a sus unidades más críticas [1].

En el caso de la Armada, este hecho se materializó en el año 2018, como una orden ejecutiva del Estado Mayor de la Armada (EMA), de dotar de un sistema de ciberdefensa a los buques en desarrollo y construcción.

El presente trabajo trata de establecer las pautas a seguir para poder diseñar efectivamente un sistema de ciberseguridad embarcable que permita ofrecer las garantías necesarias para ofrecer una defensa frente a posibles ataques cibernéticos.

2. Consideraciones previas

Lamentablemente, en el ámbito de ciberdefensa en entornos miliares, la información de partida disponible es casi nula, por lo que para el desarrollo de nuestro sistema, es necesario partir casi de cero. Tenemos constancia de que los países de nuestro entorno están trabajando en sistemas similares, pero son muy celosos de compartir información alguna al respecto. Son instalaciones muy sensibles y es normal que no se quiera compartir información.

Afortunadamente, en España existe normativa aplicable en el campo de la ciberdefensa. Está indicada especialmente para infraestructuras críticas, como pueden ser centrales nucleares o centros de control de tráfico aéreo, por ejemplo, que requieren de sistemas preventivos para garantizar un funcionamiento seguro. Dicha normativa establece reglas que se deben cumplir en dichas instalaciones, así como en las que se maneja información clasificada. Además, la acreditación de los sistemas para poder manejar dicha información es realizada por el mismo estamento, el Centro Criptológico Nacional, por lo que es un buen punto para empezar.

En nuestro caso, la información de partida incluye entre otras, la siguiente documentación:

1) Concepto de ciberdefensa militar del JEMAD (2011 y 2018)
2) Normativa STIC del Centro Criptológico Nacional (CCN) [2], [3] y [4]
3) Esquema Nacional de Seguridad, del CCN [5]

En [1] ya se marcaban las características generales que debe cumplir un sistema de ciberdefensa. Adicionalmente con el mandato del EMA referente a la inclusión de sistemas en los buques, se dejaban vislumbrar los esbozos de unos requisitos de alto nivel, que nos ayudarán a definir las capacidades y características que necesitaría un sistema válido.

Además, resulta tremendamente conveniente el definir al comienzo de un programa de desarrollo la metodología a utilizar durante el mismo. En este caso se propone la utilización de la ingeniería de sistemas como metodología de desarrollo, debido a los buenos resultados que se han obtenido en otros programas recientes, y a que en la Dirección General de Armamento y Material (DGAM) es de uso común.

La mecánica de esta metodología estriba en la definición de unos requisitos de sistema de alto nivel, sobre los que se van definiendo los sistemas primero (SDR) y los componentes después (PDR). A cada paso se va estableciendo mayor nivel de detalle. Se definen una serie de hitos para cada uno de los pasos, y no se pasa al siguiente hasta que se presenta el estado del programa en cuestión, y se aprueba por el órgano ejecutivo al cargo de su seguimiento.

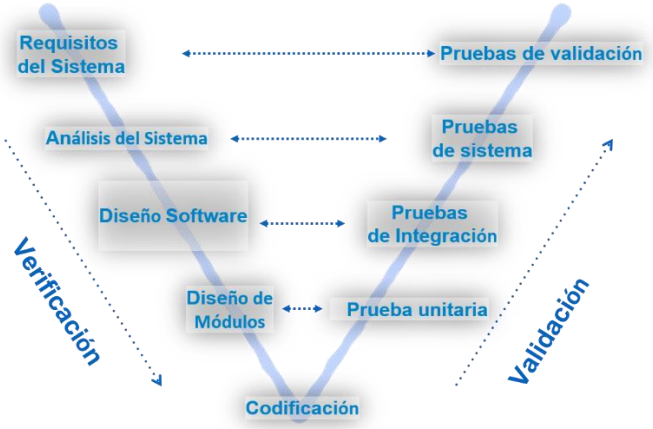

Figura 1 Modelo de desarrollo

Una vez que cerrado el diseño (CDR), empieza la fase de construcción/montaje y pruebas de componentes, hasta que el sistema completo es capaz de entrar a la fase de pruebas (TRR). En ese momento, todos los requisitos de sistemas deben ser verificados uno a uno por medio de las pruebas correspondientes, hasta llegar a verificar los requisitos de alto nivel, momento en el cual, el diseño está listo para la entrada en servicio. Este tipo de desarrollo también es conocido como desarrollo en V.

3. Requisitos del sistema

El paso siguiente propuesto tras definir la metodología, es la generación de los requisitos de alto nivel, y de los sistemas necesarios para que la configuración de nuestra propuesta sea válida.

Por lo tanto tomando de base los documentos ejecutivos y la normativa de aplicación al sistema, se crean una serie de requisitos, que nos permiten desarrollar el sistema desde ese punto.

Las características principales que el sistema debe poseer se pueden enumerar en la siguiente lista:

1) Prevenir los incidentes de seguridad informáticos.
2) Obtener la capacidad de análisis forense, para poder identificar el alcance o efectos producidos por cualquier incidente.
3) Obtener la capacidad de resiliencia.

El cumplimiento de estas características se puede traducir a necesidades de nuestro sistema de manera que:

Para el cumplimiento de 1) se propone la instalación de un sistema de colección y correlación de eventos (SIEM), que permita la generación de reglas de correlación de eventos, así como la presentación de dichos eventos al operador. También se deberán instalar sensores de tráfico de red con monitorización que permitan la detección de anomalías de red en sistemas de información con diferente grado de clasificación. Para esto se prevé la instalación de sistemas de prevención y detección de intrusos (IPS/IDS).

Para el cumplimiento de 2) la consola de seguridad tendrá capacidad de identificar el alcance real del incidente y el deterioro producido en los sistemas clasificados. La Consola de seguridad tendrá capacidad de recoger pruebas y evidencias válidas que permitan la investigación del origen y sean

admisibles en un proceso legal. Por lo tanto será necesaria adicionalmente la instalación de un sistema de almacenamiento adecuado a tal tarea.

Para el cumplimiento de 3) La Consola de Seguridad (SIEM) y los sensores asociados tendrán capacidad de operación autónoma alternativa independiente de la alimentación principal, así como sistemas de Alimentación Ininterrumpida (SAI´s) que les permitan operar aún con limitaciones eléctricas, durante al menos una hora.

Los servidores dispondrán de medios de respaldo que proporcionen capacidad de recuperación (redundancia). La arquitectura de recuperación de los servidores de respaldo debe garantizar, en caso de caída o pérdida de los servidores principales, la recuperación del sistema en un tiempo inferior a una hora.

4. Caracterización del sistema

Para poder dimensionar un sistema que cumpla con dichos requisitos, previamente hay que realizar una caracterización de los sistemas que posee nuestro "barco de pruebas", que es un barco ficticio con los sistemas más comunes existentes en los diferentes buques de la Armada.

Debido a la aplicación de la normativa CCN-STIC, es necesario realizar una división basada en el nivel de clasificación de la información que manejan las diferentes redes. En el caso de nuestro buque, se han considerado tres grados distintos de nivel de clasificación:

- Difusión Limitada, Confidencial y Reservado.

Parte del trabajo de caracterización implica determinar para cada instalación del buque, a que grupo pertenece, en la tabla 1 se recogen algunos ejemplos a modo ilustrativo.

Difusión Limitada	Confidencial	Reservado
WANPG, SICP, Red Administrativa, etc…	Red de sensores, Sistema de combate.	Sistemas de comunicaciones, mando y control.

Tabla 1 Descricpcion de redes en función de su grado de clasificación.

Tras realizar esta primera distribución, realizamos una mayor segmentación en base a los siguientes parámetros. Para las instalaciones de nuestro buque de pruebas se han identificado 5 dominios, con 15 redes distintas, a las que están conectadas 62 instalaciones, que poseen hasta 455 elementos únicos que poseen algún tipo de software. También se han identificado 7 interconexiones entre dominios. En el trabajo se realiza también una identificación del tipo de elemento por función (Pc, portátil, switches, etc.) así como de los interfaces que poseen (Ethernet, USB, teclado, serie, etc.).

Una vez realizada la composición completa de la instalación y sus dependencias, el siguiente paso es definir el valor de cada activo de buque, utilizando una valoración en base a la triada CID (Confidencialidad, Integridad y Disponibilidad), tomando como referencia las consecuencias resultantes si un elemento dado fallara por culpa de un ataque.

Una vez determinados los activos y su valoración el siguiente paso es realizar un análisis de riesgos.

5. Análisis de riesgos

Para la realización del análisis de riesgos se ha utilizado la metodología MAGERIT, que es la indicada por el CCN en sus guías STIC.

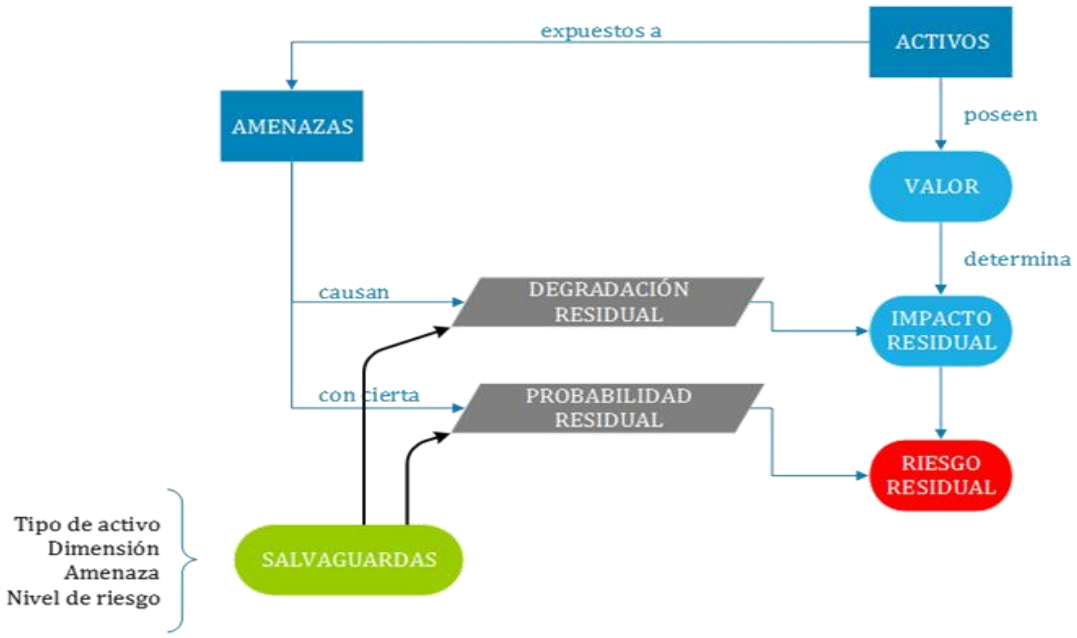

Figura 2 Metodología utilizada para el análisis de riesgos.

Esta metodología sigue el detalle mostrado en la figura 2, para la cual, una vez determinados los activos, se identifican las amenazas a las que pueden verse expuestos. Se comprueban las salvaguardas actualmente dispuestas y se determina como son de eficaces frente al riesgo potencial al que se encuentra expuesto el sistema. Se estima el impacto en caso de materialización de la amenaza. Y por último se estima el riesgo definido como el impacto ponderado con la tasa de ocurrencia de la amenaza (probabilidad y degradación).

En caso de resultar inaceptable se consideran nuevas salvaguardas con el objetivo de reducir el riesgo a un valor que hemos fijado como objetivo. La ventaja de la utilización de MAGERIT es que propone la utilización de la herramienta PILAR, la cual incluye un completo catálogo de amenazas y salvaguardas, y además proporciona cierta automatización del análisis.

Durante la realización del análisis se comparan las distintas iteraciones del mismo, hasta comprobar que el nivel de riesgo residual es aceptable tras la incorporación de las diferentes salvaguardas, quedando identificadas en el texto del trabajo.

6. Solución de diseño

Una vez determinadas las salvaguardas a nuestra propuesta queda por determinar la solución hardware y software sobre la que construir nuestro sistema.

La solución hardware se basa en 3 servidores y switches, cada uno dedicado a un dominio según el grado de clasificación. Todo el hardware debe estar alojado en un armario de dimensiones reducidas que permita su embarque. Cada uno de los servidores se encontrará redundado por una segunda unidad, dándonos un total de 6 servidores para cumplir con los requisitos de resiliencia.

Cada dominio se encuentra respaldado por una SAI. La solución software será casi en su totalidad virtualizada, por lo que se incluye un PC de gestión por sistema para su operación y administración. Además en el armario se incluyen los elementos de alimentación del mismo, así como un panel de control del sistema de ciberdefensa, una unidad de control interna y por último se incluye un KVM

común a todos los servidores para poder operar el sistema desde el propio armario. La disposición del mismo se puede observar en la figura 3.

La solución software se compone de una plataforma virtualizada con VMWare sobre la que corre el siguiente software. La aplicación SIEM, que es la encargada de recoger los registros y Logs de eventos de todo el sistema. La aplicación escogida es Q-Radar de IBM. Para el almacenamiento se ha escogido la solución Jovian DSS. Para la aplicación de detección y protección de intrusiones, así como el firewall se ha escogido Fortinet. Para la detección de amenazas basadas en el comportamiento, se ha escogido la solución de Nozomi Networks.

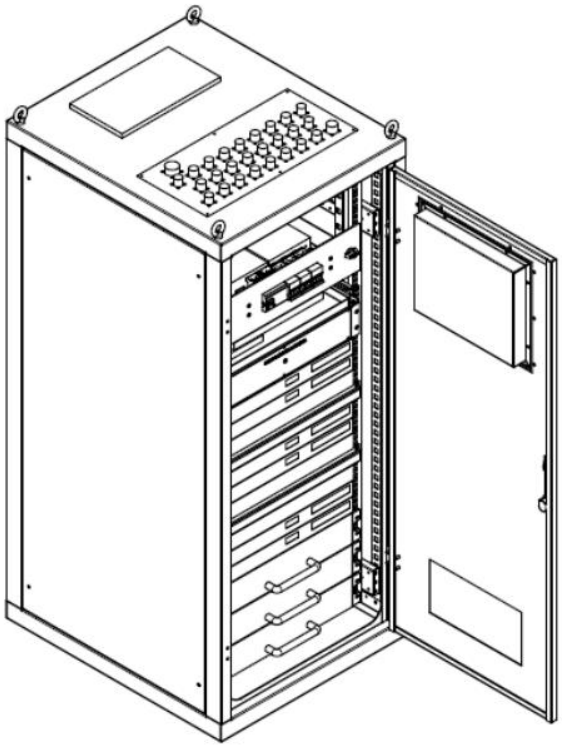

Figura 3 Disposición del armario del sistema

La adopción de estas soluciones de software por si solas no es suficiente para un correcto desempeño de las tareas de ciberdefensa para nuestro buque, ya que el sistema debe aprender las características del buque y ser entrenado conforme a los parámetros normales de funcionamiento.

Afortunadamente, todos los buques de última generación adquiridos por la Armada, han sido adquiridos a través de Navantia. El astillero público posee en cada una de sus factorías unas instalaciones llamadas LBTS (Land Based Test Site), las cuales son utilizadas para integrar los diferentes sistemas que posee cada buque, y replican la realidad de todos los sistemas conectados a bordo en tierra. La disponibilidad de este tipo de instalaciones es de gran ayuda a la hora de poder entrenar nuestro sistema de ciberdefensa, ya que éste es capaz de descubrir en el proceso las interacciones y parámetros normales de funcionamiento de todos los elementos conectados del buque. Esta base de conocimiento, una vez adquirida, formará parte de la base de datos de conocimiento necesaria para un correcto desempeño de la función de ciberdefensa a bordo de cada buque. En el trabajo se incluye así mismo una planificación del tiempo necesario para llevar a cabo dicho entreno, así como el resto de pasos antes de tener el sistema totalmente operativo.

7. Conclusiones

El presente trabajo presenta una propuesta de desarrollo de un sistema de ciberdefensa aplicable a buques de la Armada. No obstante, el sistema en sí, es una parte de lo necesario para conseguir una protección más amplia. Es igualmente necesaria la concienciación y formación del personal que opera los buques, para interiorizar las políticas implícitas que permitan reducir los riesgos de ciberataques. De igual manera, la configuración, operación, sostenimiento y explotación de estos sistemas, requerirá de personal especializado, medios y financiación adecuada a lo largo del tiempo, por lo que se deberían asegurar estos tres elementos para conseguir la más amplia protección posible en los buques de la Armada de manera continuada en el tiempo.

8. Referencias

[1] Jefe del Estado Mayor de la Defensa (JEMAD), Concepto de Ciberdefensa Militar, 2011.

[2] Centro Criptológico Nacional, CCN-STIC-301 Medidas de Seguridad de las TIC a Implementar en Sistemas Clasificados, 2020.

[3] Centro Criptológico Nacional, CCN-STIC-302 Interconexión de CIS, Julio 2012.

[4] Centro Criptológico Nacional, CCN-STIC-303 Inspección STIC, Enero 2009.

[5] Centro Criptológico Nacional, «Esquema Nacional de Seguridad,» Enero 2022. [En línea]. Disponible: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1003.