Documento de Trabajo
03/2017

Plan anual de investigación 2017

Organismo solicitante del estudio:

Escuela Superior de las Fuerzas Armadas (ESFAS)

Protección de elementos esenciales de información propia en un Área de Operaciones de Ciberdefensa

Protección de elementos esenciales de información propia en un Área de Operaciones de Ciberdefensa

Maquetado en mayo de 2017 por el Instituto Español de Estudios Estratégicos (IEEE)

Centro Superior de Estudios de la Defensa Nacional (CESEDEN)

Índice

Anexos

Índice de tablas

Protección de elementos esenciales de información propia en un Área de Operaciones de Ciberdefensa

Félix Nieto Ortega
Comandante de Infantería de Marina
Analista Estado Mayor Conjunto

Resumen

La enorme expansión de las tecnologías de la información y las comunicaciones a lo largo de los últimos años ha ido en paralelo al desarrollo de herramientas para explotar sus vulnerabilidades.

Dado que no es posible proteger toda la información sensible que circula por los sistemas de información propios, es necesario establecer procedimientos que permitan asignar mayores recursos en seguridad allí donde sea más necesario.

A lo largo de la presente investigación se demuestra que el proceso de Seguridad de las Operaciones (OPSEC) y la valoración de riesgos adaptados al dominio ciberespacial es un método válido para gestionar de manera eficiente la protección de los elementos esenciales de información propia en un nuevo terreno: el Área de Operaciones de Ciberdefensa (AOCD).

Palabras clave

Ciberdefensa, seguridad de la información, análisis de riesgos, seguridad de las operaciones, EEFI.

Abstract

The enormous expansion of information and communication technology over recent years has evolved in parallel to the development of tools to exploit their vulnerabilities.

Since it is not possible to protect all sensitive information flowing through own information systems, it is necessary to establish procedures that allow allocate more security resources where they are most needed.

Throughout this investigation, I try to demonstrate that the process of Operations Security (OPSEC) and risk assessment adapted to cyberspace domain is a valid method to efficiently manage the protection of the essential elements of friendly information in a new ground: Cyber Defense Operations Area (CDOA).

Keywords

Cybersecurity, information security, risk assesment, OPSEC, EEFI.

Introducción

«Cyber-attacks are the greatest

transfer of wealth in human history».

U.S. Cyber Command.

Planteamiento del problema

Durante la ejecución de las operaciones militares, hay cierta información, generalmente relacionada con las intenciones, capacidades y actividades propias, que debe ser protegida con especial atención. Y ello es así porque, en caso de ser revelada al enemigo, podría hacer peligrar el cumplimiento de la misión. Son los conocidos como «elementos esenciales de información propia» (EEFI por sus siglas en inglés)[1].

La determinación correcta de los EEFI es esencial para alcanzar un buen grado de Seguridad de las Operaciones (OPSEC). Independientemente del tipo de operación que se lleve a cabo, una parte importante de los EEFI se encontrarán almacenados en los sistemas de información empleados por la Fuerza. Y en su protección, desempeñará un papel preponderante la **ciberdefensa**, definida como «*la aplicación de medidas de seguridad para proteger los componentes de la infraestructura de los sistemas de información y comunicaciones contra las ciberamenazas*»[2].

Durante el desarrollo de operaciones militares conviven generalmente redes informáticas por las que discurren datos sin clasificar con sistemas de información acreditados para el manejo de información clasificada. Estos últimos deben cumplir una serie de requisitos de seguridad que serán más exigentes cuanto mayor sea el grado de seguridad de la información que pretendan manejar.

La existencia de sistemas acreditados para el manejo de datos clasificados no implica que los elementos esenciales de información propia se encuentren siempre contenidos en ellos.

1 El acrónimo corresponde a «Essential Elements of Friendly Information». NATO STANDARDIZATION AGENCY «AAP-15 NATO Glossary of abbreviations used in NATO documents and publications». Mayo 2014.

2 Definición extraída del NATO MC 0571 «NATO Cyber Defense Concept». Febrero 2008.

La adecuada identificación de los EEFI en cada situación particular y su localización en la arquitectura de los sistemas de información que participan en la operación es de enorme valor para todos aquellos órganos con responsabilidades en la seguridad de la información.

Solo así se podrán gestionar los recursos dedicados a la seguridad de la información en los sistemas de información y telecomunicaciones de forma eficiente.

Para la redacción del presente documento se han usado referencias doctrinales tanto nacionales como de la OTAN. Concretamente, de aquellas publicaciones relacionadas con la determinación de los requisitos de intercambio de información en operaciones, protección de la fuerza y operaciones de información.

Sin embargo, dado la característica del documento, para publicar en la página web del Instituto Español de Estudios Estratégicos, se ha optado por evitar referencias a documentación clasificada, incorporando fuentes de acceso público que cumplen de igual manera con el objetivo de la investigación. Es el caso de las clasificaciones utilizadas para valorar el riesgo en el ciberespacio o la taxonomía de las amenazas cibernéticas.

En estos casos, se han sustituido los documentos clasificados, por estándares comerciales relacionados con seguridad de la información y gestión del riesgo en los sistemas de información del *National Institute of Standars and Technology del U.S. Deparment of Commerce*.

Se ha optado por tomar como referencia estos estándares por su vigencia, su carácter «sin clasificar» y por su importancia como referencia en el área de la seguridad de la información a nivel mundial[3].

Otro aspecto a considerar es la valoración del riesgo, que va a jugar un papel preponderante dentro del proceso OPSEC. Y ello es así por varios motivos:

- En primer lugar, para evitar la búsqueda de una utopía: la protección de toda la información contra todas las amenazas. La enorme cantidad de información que se maneja en las operaciones actuales a través de los sistemas de información hace imposible mantener un elevado nivel de protección para toda aquella información que podríamos considerar sensible.
- En segundo lugar, para evitar la sobreprotección de información de escasa importancia y la desprotección de información sensible. Se trata de identificar

3 Son los estándares de referencia empleados en algunos de los cursos impartidos por la *University of Washington* y a los que ha tenido acceso el autor, como son el «Designing and executing information security strategies» (agosto-noviembre 2014), «Building an information risk management toolkit» (agosto-noviembre 2014) y «Information security and risk management in context» (enero-marzo 2013).

qué elementos tenemos que proteger y buscar la eficiencia a la hora de implementar medidas de protección de la información en nuestros CIS.

El estudio está influenciado por las nuevas tendencias en el ámbito OTAN, como el *Federated Mission Networking* (FNM), que permitirá mejorar la capacidad de instalar de forma rápida redes informáticas para una misión concreta, mejorando la interoperabilidad y el intercambio de información entre los actores participantes en la operación.

El FNM cambiará la forma de ver los sistemas de información y telecomunicaciones en operaciones como elementos aislados por otro en el que diferentes redes, incluida internet, se interconectan entre sí usando una serie de políticas, procedimientos y estándares comunes.[4]

Este nuevo paradigma, hará converger los CIS de las futuras operaciones que lleve a cabo la OTAN con el ciberespacio, entendido este como el «dominio global y dinámico compuesto por las infraestructuras de tecnología de la información –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones»[5]. Por lo tanto, para facilitar el análisis y obtener resultados válidos en este nuevo entorno CIS que conformará el FNM, se propone la definición de un nuevo concepto: el Área de Operaciones de Ciberdefensa (AOCD) como:

«Conjunto de infraestructuras de tecnología de la información, las redes y los sistemas de información y telecomunicaciones que intervienen en el planeamiento y ejecución de una misión de nivel operacional y que es necesario proteger debido a la sensibilidad de la información que manejan.»

Dada la amplitud del campo de investigación, se ha decidido limitarlo al nivel operacional por varios motivos. En primer lugar, porque es un nivel especialmente complejo desde el punto de vista de los sistemas de información y telecomunicaciones, pues es el que hace de enlace entre los niveles estratégico y táctico.

Y segundo, por la equivalencia conceptual que se pretende establecer entre el concepto de Área de Operaciones de Ciberdefensa (AOCD) y la *Joint Operation Area* (JOA) de la OTAN.

Así mismo, se considera necesario aclarar el significado de algunos de los conceptos que se repiten a lo largo del documento. Se trata de tres características de la información: sensibilidad, criticidad y confidencialidad. A lo largo del texto, el sentido de dichas características es el siguiente:

4 NATO ALLIED COMMAND TRANSFORMATION. «Federated Mission Networking (FMN)». Febrero 2015. Disponible en www.act.nato.int/fmn (fecha de la consulta: 09.04.2016).

5 GOBIERNO DE ESPAÑA. «Estrategia de Ciberseguridad Nacional». 2013. Pág 9.

Sensibilidad de la Información: medida de la importancia asignada a la información por una organización con el fin de destacar la necesidad de su protección para el cumplimiento de la misión.[6]

Criticidad de la Información: Medida del grado en el cual una organización depende de determinada información o de un sistema de información para el éxito de su misión.

Confidencialidad de la Información: preservación de las restricciones impuestas al acceso y divulgación de información.

Las redes y sistemas de información en el AOCD

El intercambio de información en operaciones

La doctrina CIS de la Alianza define «mando» como un proceso mediante el cual la decisión e intenciones de un comandante se trasladan a las unidades subordinadas. El mando incluye la autoridad y responsabilidad sobre las fuerzas desplegadas para el cumplimiento de la misión[7].

El «control», por otra parte, es el proceso mediante el cual el comandante, asistido por su Estado Mayor, organiza, dirige y coordina las actividades de la fuerza puesta bajo su mando[8]. Para conseguir que ambos procesos funcionen correctamente en el nivel operacional, el comandante y su Estado Mayor usan procedimientos estandarizados y sistemas de información y telecomunicaciones (CIS). Ambos constituyen el sistema de mando y control que se empleará para planear, dirigir, coordinar y controlar las operaciones.

El objetivo y la escala del apoyo CIS al mando y control se determina por una combinación de estructura organizativa, dispersión geográfica y **necesidad de intercambio de información** entre las principales entidades de mando y control.

6 Según la Norma NS/04 de la Autoridad Nacional para la Protección de la Información Clasificada, información sensible es cualquier información o material respecto del cual se decida que requiere protección contra su divulgación o acceso no autorizados, con independencia de que se le haya asignado o no una clasificación de seguridad.

7 NATO STANDARDIZATION AGENCY. «AJP-6 Allied Joint Doctrine for Communication and Information Systems». Abril 2011, pág 1-7.

8 Ibídem.

Por su importancia a lo largo de la presente monografía, en el siguiente apartado se describe cómo se determinan los **requisitos de intercambio de información**[9] (IER por sus siglas en inglés) para una operación determinada.

Requisitos de intercambio de información

Según la doctrina OTAN en vigor, aquella información que debe ser intercambiada entre unidades operativas para proporcionar a los comandantes la información esencial para la toma de decisiones, se conoce como los «requisitos de intercambio de información»[10].

La transferencia de esta información entre los Cuarteles Generales, la Fuerzas y demás organizaciones que, de alguna forma están involucradas en el planeamiento y ejecución de las operaciones, es vital para el cumplimiento de los objetivos de cada una de ellas.

Los responsables de la toma de decisiones necesitan sistemas de información para el mando y control (C2IS) que les permita obtener esa información esencial o bien ponerla a disposición de otros órganos.

Los IER ponen de relieve la necesidad de compartir información de las entidades de mando y control de una operación y la conectividad CIS necesaria a lo largo de la operación.

Hay diferentes clases de IER en función del tipo de operación que se vaya a ejecutar. Una gran parte de ellos podría asociarse a alguna de las siguientes categorías[11]:

- Órdenes, directivas y planes.
- Conocimiento de la situación, incluyendo fuerzas amigas, enemigas y neutrales y la información ambiental, incluida la meteorológica.
- Medidas de control.

9 Corresponde al acrónimo OTAN para los «information exchange requirements». NATO STANDARDIZATION AGENCY. «AAP-15 NATO Glossary of abbreviations used in NATO documents and publications». Mayo 2014.

10 «*Those categories of information that must be exchanged between operational facilities to provide commanders with essential information for decision-making*». NATO STANDARDIZATION AGENCY «AJP-6 Allied Joint Doctrine for Communication and Information Systems». Abril 2011: LEX-4.

11 Clasificación obtenida del documento NATO INTERNATIONAL MILITARY STAFF MC 0593 «Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations». Febrero 2015.

- Información sobre los Sistemas de Información y Comunicaciones (CIS) y los Apoyos de Servicio de Combate (CSS).
- Informes.
- Información referente a áreas funcionales tales como artillería, ingenieros, aviación y otros.

La definición de los IER son claves para el proceso de planeamiento CIS. Una vez identificados, se debe asegurar que se pueden proporcionar de manera adecuada.

En el proceso de identificación de los IER participan todas las secciones del Estado Mayor. Una vez determinados, la Sección J6 estará en disposición de diseñar el núcleo de la estructura CIS, determinando que sistemas de información y qué conexiones necesita cada organismo para el planeamiento y ejecución de la operación.[12]

La definición de un IER incluye generalmente información sobre el nivel de clasificación necesario y el tipo de servicio. Entre estos últimos, los servicios funcionales son herramientas que proporcionan apoyo a una función específica.

Un servicio funcional podría ser una herramienta de apoyo a la decisión, una herramienta de planeamiento o cualquier otro tipo de capacidad requerida por un Estado Mayor, generalmente orientado hacia una función específica, como inteligencia o logística.

Determinación de sistemas a desplegar en una operación

Una vez que los IER se han determinado por el nivel operacional, el comandante debe producir la matriz de servicios funcionales en coordinación con los comandantes subordinados y con el nivel estratégico. La matriz incluye entre otros el tipo de servicio, la localización donde debe ser proporcionado, y la red por la que debe funcionar.

Una vez hecho esto, el diagrama de los servicios funcionales proporciona una explicación gráfica de los servicios proporcionados, la conectividad necesaria para ello y las funciones de cada usuario del servicio funcional.

Con la información anterior, ya se está en disposición de establecer las necesidades de sistemas de información y telecomunicaciones a desplegar.

El método descrito hasta el momento, está tomando una nueva dirección a raíz de las experiencias adquiridas en Afganistán por la *International Security Assistance Force* (ISAF).

12 En el ANEXO A muestra un diagrama de servicios de nivel Cuartel General operacional.

La puesta en práctica del concepto NATO *Network Enable Capability*[13] (NNEC) a través de la *Afghanistan Mission Network* (AMN) fue identificado como el enfoque necesario para el futuro de las estructuras CIS en operaciones y el concepto se institucionalizó como *Federated Mission Networking* (FMN).

A través del FMN, se buscará unificar las redes y sistemas que proporcionan servicios de intercambio de información en una operación de forma que se permita compartir datos entre todos aquellos actores que participen en una misión a través de una misma estructura CIS a la cual se podrán federar siempre y cuando cumplan con los requisitos establecidos para dicha red.[14]

Los EEFI como requisito de intercambio de información

Como se ha visto en los apartados anteriores, para definir la arquitectura CIS de una operación, lo primero que hay que establecer es qué información tiene que ser intercambiada entre los organismos que participan en una operación militar y que proporcionarán a los comandantes la información esencial para la toma de decisiones.

Si tratamos de meternos en la piel de un posible adversario que trate de oponerse a nuestra misión, no toda esta información tendrá la misma relevancia. Por ello, de lo que se trata ahora es de identificar qué parte de esta información debe ser especialmente protegida puesto que de ser conocida por el enemigo podría poner en riesgo el cumplimiento de la misión. En definitiva, se trata de determinar qué parte de esta información, contenida en los CIS, debe ser clasificada como «elementos esenciales de información propia».

Identificación de los EEFI

En el caso que nos ocupa, la información sensible se corresponde con aquellas cuestiones que un adversario se pregunta sobre las intenciones, capacidades y actividades propias y que, de ser respondidas, le proporcionarán una posición de ventaja para para oponerse con efectividad al cumplimiento de nuestra misión.

13 Entendido como la «*capacidad técnica y cognitiva de la Alianza para federar varios componentes del entorno operacional, desde el nivel estratégico hasta el táctico, a través de infraestructura de redes e información*» NATO MCM-0032-2006, «NATO Network-Enabled Capability (NNEC) Vision and Concept». Abril 2006.

14 NATO ALLIED COMMAND TRANSFORMATION. «Federated Mission Networking (FMN)». Febrero 2015. Disponible en línea en www.act.nato.int/fmn (fecha de la consulta: 09.04.2016).

La determinación de los EEFI lleva consigo la identificación de aquellos elementos de información que puedan revelar aspectos relacionados con las fuerzas propias que se consideran imprescindibles para alcanzar el éxito de la misión. Ello debe dar como resultado un listado valorado de la información que, si se divulga o resulta accesible al adversario, podría comprometer el éxito de la misión. Esto permitirá más adelante priorizar nuestros esfuerzos de seguridad CIS.

Ejemplos de EEFI para una operación genérica pueden ser los siguientes[15]:

- Fuerzas disponibles, objetivos y calendario.
- Tácticas técnicas y procedimientos.
- Capacidades logísticas y limitaciones.
- Nodos de comunicaciones críticos.
- Planes de Operaciones.
- Disposición de Fuerzas y composición de la reserva.

Los EEFI pueden ser manejados por una o varias áreas funcionales. Por esta razón, es importante que todas las secciones del Estado Mayor se involucren en el proceso de identificar cuáles podrían ser sus EEFI.

En la doctrina OTAN[16] es la célula Info Ops la responsable de identificar los EEFI, principalmente en la fase de análisis de la misión. Además, también es una de sus funciones la realización de una valoración inicial del riesgo, desde el punto de vista de su área de trabajo.

Los CIS como EEFI

El correcto desarrollo de las operaciones militares depende en muy alto grado de los CIS. Tanto es así que ciertos aspectos relacionados con estos sistemas podrían ser considerados en sí mismos «elementos esenciales de información propia».

A través del conocimiento de los activos que componen un sistema de información y telecomunicaciones, un adversario podría realizar acciones que impidiesen su uso por parte de las fuerzas propias y como consecuencia, se impidiese el cumplimiento de la misión.

15 U.S. Joint Publication 3-13.3 «Operations Security» Enero 2012, pág II-3.

16 NATO STANDARDIZATION AGENCY «AJP-3.10 Allied Joint Doctrine for Information Operations, Ed A, ver 1». Diciembre 2015, pág. 3-11.

Por lo tanto, si el cumplimiento de la misión depende del uso de los CIS y el adversario tiene capacidad para negar su uso por parte de las fuerzas propias, debemos considerar a los CIS como EEFI.

Pero obviamente, al igual que no toda la información clasificada son EEFI, no todos los CIS van a ser considerados elementos esenciales de información propia. Para determinar qué parte de los sistemas tiene que ser protegida con especial atención frente a la inteligencia enemiga, una opción útil podría consistir en la identificación del «**terreno clave**» en un AOCD tal y como se hace en la doctrina terrestre.

Generalmente, se considera «terreno clave» a la porción de espacio físico que una vez controlada, proporciona una significativa ventaja sobre el adversario. Trasladado al ciberespacio, el terreno clave incluiría aquella infraestructura de tecnología de las comunicaciones y de la información que se considera crítica para el desarrollo de una misión.

En este proceso, será necesario identificar los riesgos inherentes al conocimiento por parte del adversario de nuestros activos CIS y priorizar aquellos que deben ser protegidos con especial atención.

Estos activos tienen vulnerabilidades que podrían ser explotables por una amenaza en particular y pueden ser de varios tipos:

- **Hardware: T**odos aquellos elementos físicos que apoyan a los procesos de la información. Incluye entre otros, los equipos portátiles, servidores, periféricos y dispositivos de almacenamiento de datos.

- **Software: E**l software consiste en todos aquellos programas que contribuyen al procesado de los datos. Entre ellos se contemplan los sistemas operativos, el software de servicio mantenimiento y administración o aquellas aplicaciones específicas que ha sido específicamente desarrolladas para proporcionar a los usuarios acceso a los servicios y funciones que requieren de un sistema de información.

- **Red:** Aquellos los dispositivos de telecomunicaciones usados para interconectar varios ordenadores o elementos de un sistema de información físicamente distantes entre sí. Puede estar determinado por las características técnicas y físicas de los equipos de telecomunicaciones, por los protocolos, dispositivos intermedios (*bridge, router, hub, switch*) o por los interfaces de comunicaciones (GPRS, *Ethernet,* etc…).

- **Personal:** Consiste en todos los grupos de personas involucrados en un sistema de información: usuarios, administradores, operadores, mantenedores, desarrolladores etc…

- **Instalaciones:** Incluye todos aquellos lugares que contienen los activos antes descritos y los medios físicos necesarios para operarlos.

Una vez realizado el inventario de todos los activos que componen los CIS, es necesario valorar qué impacto tendría sobre la misión el conocimiento de cada uno de los activos por parte del adversario. Ello va a depender del escenario en el que se desarrolle la operación. Diferentes amenazas producirán diferentes impactos en los activos.

Además, es necesario estimar la probabilidad de que una amenaza se materialice y la probabilidad de resultar en impacto sobre los activos. El resultado de dichos valores determinará el nivel de riesgo en un escenario concreto, pudiendo dar como resultado la **«tabla I»**.

Tabla I

Sistema	Hardware	Software	Red	Personal	Instalaciones
Sistema A	Alto	Muy Alto	Muy Alto	Alto	Alto
Sistema B	Medio	Alto	Alto	Medio	Medio
Sistema C	Medio	Medio	Medio	Medio	Medio
Sistema D	Bajo	Medio	Medio	Bajo	Bajo
Sistema D	Bajo	Bajo	Bajo	Bajo	Bajo

Tabla I: Riesgo estimado para los componentes de un sistema de información. (Fuente: elaboración propia).

En este proceso, y al objeto de reducir el riesgo en cada uno de los sistemas de información, es necesario tener en cuenta los conceptos de *segmentación*, *redundancia* y eliminación de los *puntos únicos de fallo*[17].

La **segmentación** permite separar funciones de los sistemas de información y componentes o subsistemas que apoyen a los sistemas principales. Ello reduce el grado de impacto que pueda provocar una amenaza que explote las vulnerabilidades existentes.

Cuando existe una alta probabilidad de que una amenaza explote alguna de las vulnerabilidades propias, la degradación de uno o más sistemas de información es inevitable. Para mejorar la resiliencia de un sistema de información como parte de la respuesta al riesgo, la **redundancia** permite que los componentes atacados desencadenan el funcionamiento de otros componentes con capacidades similares que aseguran así la continuidad en el funcionamiento del sistema.

Por último, hay que tener especial consideración los conocidos como **puntos únicos de fallo**. Estos son componentes de un sistema que tras un fallo en su funcionamiento ocasionan un fallo global en el sistema completo, dejándolo inoperante. Para garantizar

17 U.S. DEPARTMENT OF COMMERCE. National Institute of Standards and Technology «NIST 800-39 Managing Information Security Risk». Marzo 2011, pág 19.

que no existan estos puntos, todos sus componentes deben ser duplicados, conformando así un sistema de alta disponibilidad que garantice el correcto funcionamiento aún en caso de que alguno de sus componentes falle.

La defensa de los EEFI en un AOCD

El entorno operacional y el ciberespacio

El entorno operacional abarca condiciones, circunstancias e influencias que afectan al empleo de las capacidades militares y a las decisiones de cualquier comandante operacional.[18] La comprensión de este entorno, en el cual se llevarán a cabo las operaciones militares, requiere de una visión integral que incluya factores físicos, políticos, militares, económicos, socio-culturales, de infraestructura y del entorno de la información.

Con la emergencia del ciberespacio, este se ha convertido en parte de cada uno de estos factores que definen el entorno operacional. El ciberespacio no posee fronteras claras y no tiene en cuenta necesariamente las fronteras geográficas y físicas entre estados. En consecuencia, es complejo definir el área de operaciones del dominio ciberespacial.

El Área de Operaciones (AOO), como delimitación física, incluye la infraestructura que afecta al desarrollo de la operación. Sin embargo, cuando se habla de amenazas cibernéticas, estas pueden proceder bien del interior del Área de Operaciones física, bien de un área alejada de ella. Los actores hostiles que actúan en el ciberespacio no se ven constreñidos a atacar a la Fuerza desde el interior del AOO. El Área de Operaciones en su dimensión ciberespacial, siempre será mayor que la referente a los dominios físicos.

Por otra parte, el **Área de Interés (AI)**, que se define como el «*área que concierne a un comandante en relación con la consecución de los objetivos de las operaciones en curso o planeadas*»[19], incluye también aquella ocupada por fuerzas enemigas que podrían poner en peligro el cumplimiento de la misión[20].

18 NATO STANDARDIZATION OFFICE. «AAP-6 NATO Glossary of terms and definitions». 2015.

19 Ibídem.

20 U.S. Joint Publication 1-02 «Dictionary of Military and Associated Terms». 2013.

En consecuencia, cuando se trata de considerar los lugares desde donde se puedan originar ciberataques, es fácil imaginar que el «**Área de Interés de Ciberdefensa**» **(AICD)** debe ser bastante mayor que el AOO y el AI para los dominios físicos.

Los ciberataques se pueden llevar a cabo prácticamente desde cualquier lugar y en cualquier momento, lo que incrementa la dificultad de determinar las fronteras geográficas para el AICD.

Por lo tanto, en lugar de definir bordes geográficos para establecer una AICD, tiene más sentido definir un escenario en función de los actores y sus intereses en el conflicto.

Es por ello que, en el estudio del entorno operacional, hay una serie de necesidades de información relacionadas con los actores adversarios que deben ser resueltas para lograr un conocimiento adecuado del ambiente cibernético en el que se va a desarrollar la operación. Estas pueden incluir algunas de las siguientes:

- ¿Qué actores están presentes o tienen algún interés en el Área de Operaciones de Ciberdefensa?
- ¿Cuáles son sus intenciones?
- ¿Cuáles son sus capacidades?
- ¿Han realizado ciberataques o cualquier otra operación cibernética ofensiva con anterioridad?
- ¿Qué organizaciones gubernamentales y no gubernamentales toman parte en actividades relacionadas con el ciberespacio?

Definición de escenarios en un AOCD

En la doctrina nacional conjunta (PDC-01) se usa el concepto de «intensidad del entorno» como el nivel de oposición militar, o de violencia organizada, presente en una zona de operaciones. Este nivel de oposición va a contribuir a dar forma escenario en el que se desarrollarán las operaciones.

Así, en los entornos de *alta intensidad*, la oposición militar está organizada, con capacidades complementarias y coordinadas, adecuadas para el entorno. En ellos predominan las operaciones de combate convencional, aunque estas pueden combinarse con acciones de tipo asimétrico.

En los entornos de *media intensidad*, existe oposición de tipo militar, pero no está eficazmente organizada y coordinada.

Puede producirse una alternancia entre operaciones convencionales limitadas y no convencionales, con predominio normalmente de estas últimas.

Finalmente, en los entornos de *baja intensidad,* no existe una oposición militar organizada, pero sí pueden desarrollarse situaciones de violencia esporádica por parte de grupos armados o terroristas y se realizan principalmente operaciones para garantizar la libertad de acción propia frente a amenazas no convencionales.

Esta clasificación, aunque útil para un tipo de planeamiento militar convencional, tiene pocas ventajas si lo que tratamos de evaluar es la intensidad del entorno en un Área de Operaciones de Ciberdefensa. En ella, se podrían encontrar escenarios muy exigentes sin que necesariamente se lleven a cabo operaciones de combate convencional en el resto de dominios.

En un AOCD en la que existen actores adversarios que tratan de obtener información de nuestros sistemas, las amenazas se materializarán generalmente a través de capacidades ciberespaciales, entendidas como dispositivos, programas informáticos, o técnicas designados para crear un efecto en o a través del ciberespacio.[21]

Por ello, para el establecimiento de escenarios, se considera más oportuno definir en primer término el tipo de actores presentes en el entorno operacional con intención de oponerse a la misión propia a través de la obtención de nuestros EEFI en el AOCD.

Además, los actores probablemente conducirán actividades en el ciberespacio antes de cualquier conflicto para recolectar información que posteriormente le proporcionarán una posición de ventaja para poder llevar a cabo ciberataques durante el desarrollo del conflicto.

Así, los actores adversarios podrían estar clasificados en cinco categorías basadas en sus respectivas capacidades de realizar operaciones en el ciberespacio y sus tácticas, técnicas y procedimientos (TTP):

- **Actores de amplio alcance**. Actores que disponen de expertos y capacidades para llevar a cabo espectro completo de operaciones en el ciberespacio. Puede llevar a cabo ciberataques múltiples, continuos y coordinados.
- **Actores desarrolladores de programas**. Actores con amplio acceso a tecnologías de la información a través de la industria. Desarrollan programas para operar en el ciberespacio y poseen capacidades de espionaje tradicional. Pueden generar oportunidades que propicien la realización de ciberataques múltiples y coordinados.
- **Actores capaces**. Actores que poseen capacidades de espionaje tradicional y capacidades de desarrollar operaciones en el ciberespacio. No disponen de los

21 U.S. «Joint Publication 3-12. Cyberspace Operations». Febrero 2013, pág I-6.

recursos para de los actores desarrolladores de programas. Se centran en accesos remotos y denegación de servicio.

- **Actores con capacidad de acceso remoto**. Estos actores pueden acceder a sistemas conectados a internet mediante el uso de herramientas disponibles de fuentes abiertas, pero no disponen de capacidad de espionaje tradicional. Tienen capacidad limitada para generar las oportunidades que apoyen la realización de un ciberataque.
- **Actores independientes**. Actores con acceso a expertos en hardware y software pero que no muestran evidencias de llevar a cabo operaciones en el ciberespacio o actividades de espionaje tradicional. Capacidad muy limitada para generar oportunidades que apoyen la realización de un ciberataque.

La presencia de uno o más de estos actores en un AOCD va a configurar una serie de amenazas que determinarán el escenario en el que se va a desarrollar la operación.

Para el desarrollo de la presente investigación, las capacidades que más interesan son aquellas que permiten a un actor hostil la obtención de información sensible de nuestros sistemas de información y telecomunicaciones.

Por lo tanto, dado su posterior interés para llevar a cabo la valoración de riesgos, se describen en el ANEXO B una serie de escenarios ordenados de forma creciente en cuanto a la capacidad del adversario para acceder a la información contenida en un AOCD.

La protección de la información en el AOCD

Los nuevos conceptos como el *Federated Mission Networing* de la OTAN, van a precisar de un nuevo enfoque para afrontar la defensa de la información contenida en las «redes de misión» o «mission networks».

Parece que, a nivel operacional, la instalación de redes aisladas tiene cada vez menos sentido al no propiciar el intercambio de información de acuerdo al nuevo paradigma de «necesidad de compartir». Por ello es necesario definir conceptualmente el conjunto de redes y sistemas de información y telecomunicaciones que es necesario defender en un entorno operacional influenciado por el ciberespacio.

A efectos de la presente monografía, se busca identificar las redes que debemos proteger para que, entre otras cosas, la información en ellas contenida no sea accesible a usuarios no autorizados.

Así, se ha definido en la introducción del presente documento el **Área de Operaciones de Ciberdefensa (AOCD)** como el *«conjunto de infraestructuras de*

tecnología de la información, las redes y los sistemas de información y telecomunicaciones que intervienen en el planeamiento y ejecución de una misión de nivel operacional y que es necesario proteger debido a la sensibilidad de la información que manejan».

Este marco conceptual permitirá centrar los esfuerzos y delimitar las responsabilidades a la hora de proteger la información en los CIS.

En este sentido, los esfuerzos en ciberdefensa pueden dividirse en dos categorías: reactivos y proactivos[22]. La ciberdefensa reactiva trata de detectar operaciones ofensivas en el ciberespacio cuando tienen lugar, y entonces buscan mitigar sus efectos. Por otra parte, la ciberdefensa proactiva depende bastante de la inteligencia disponible y busca identificar y manejar las amenazas antes de que se introduzcan en nuestros sistemas de información.

En una AOCD, la ciberdefensa se dividirá normalmente en cuatro fases: prevención, detección, absorción y recuperación[23]:

- **Fase de prevención:** Es la que trata de disuadir a los posibles atacantes de ejecutar ataques y reducir vulnerabilidades antes de que un ataque sea desencadenado para mitigar los efectos.
- **Fase de detección:** Busca detectar y manejar los ataques de la manera más efectiva posible, tratando de obtener al mismo tiempo información que facilite su análisis y la atribución.
- **Fase de absorción:** En esta fase se intenta reducir los daños que puedan producirse como resultado de un ataque tratando de retardar y hacer menos efectivas las acciones del atacante.
- **Fase de recuperación:** Durante esta fase, se tratará de volver rápidamente a la estabilidad tras el ataque que se haya sufrido.

A lo largo del siguiente capítulo, se tratará de forma extensiva como afrontar la primera fase mediante el proceso de Seguridad de las Operaciones y la gestión del riesgo.

22 ENDRESEN, Ragnhild et al. «Handbook for integrating CyberDefense into the OPP»(NU) *Multinational Capability Development Campaign* (MCDC). 2014, pág 27.

23 Ibídem.

Protección de los EEFI a través del proceso OPSEC

Los EEFI y la gestión del riesgo

Las tecnologías de la información y las comunicaciones proporcionan una ventaja crucial a aquellos actores que consiguen utilizarlas en su favor y denegar su uso al adversario. Las organizaciones dependen cada vez más de los sistemas de información para llevar a cabo con éxito sus misiones.

Sin embargo, estos están expuestos a amenazas que pueden tener como resultado el compromiso de la confidencialidad, integridad o disponibilidad de la información mediante la explotación de vulnerabilidades.

La protección de los elementos esenciales de información propia tiene que ver con la confidencialidad. Puesto que no es posible la «seguridad total», es necesario concentrar los esfuerzos defensivos en proteger aquella información que, de ser conocida por el adversario, pondría en peligro el cumplimiento de la misión.

Tradicionalmente, los sistemas de información y comunicaciones se han dividido entre aquellos acreditados para manejar información clasificada[24] y aquellos que no lo están. Es una división basada en el grado de clasificación de seguridad de la información que están autorizados a tratar. Ello permite centrar los esfuerzos de protección en aquellos sistemas que manejan información de mayor grado de clasificación.

Sin embargo, aunque toda la información clasificada es sensible, no toda la información sensible es información clasificada. Dado que no es posible proporcionar el mismo nivel de protección a toda la información que se maneja en los CIS, es necesario implementar procedimientos que permitan gestionar eficientemente la protección de aquella información que hayamos identificado como «más sensible».

De ahí que sea absolutamente necesario gestionar el riesgo asociado con el uso de los sistemas de información que contienen elementos esenciales de información propia.

24 Según la Orden Ministerial 76/2006 de 19 de mayo por la que se aprueba la política de seguridad de la información del Ministerio de Defensa, información clasificada son todos aquellos asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puedan dañar o poner en riesgo la seguridad y defensa del Estado o afectar a la seguridad del Ministerio de Defensa, amenazar sus intereses o dificultar el cumplimiento de su misión.

Los comandantes deberán tomar decisiones para equilibrar los beneficios obtenidos del empleo de estos sistemas de información con el riesgo de que se conviertan en vehículos a través de los cuales se realicen ataques para la obtención de información sensible.

Mediante la gestión del riesgo en los sistemas de información, se debe proporcionar las necesarias medidas para proteger los EEFI en los sistemas de información y, por ende, el cumplimiento de la misión.

A lo largo de la presente monografía, se propone que las decisiones basadas en la valoración del riesgo sean tomadas como parte del proceso de Seguridad de las Operaciones.

La seguridad de las operaciones en el AOCD

La Seguridad de las Operaciones se define como el proceso que procura la apropiada seguridad a una operación militar o ejercicio, mediante el empleo de medios activos o pasivos para denegar al enemigo el conocimiento de la disposición, capacidades e intenciones de las fuerzas propias.[25]

OPSEC identifica y protege información que es de importancia vital para el éxito de una operación y que se conoce como *elementos esenciales de información propia*. A través del proceso OPSEC, se mitigan los riesgos asociados con vulnerabilidades específicas para denegar a la inteligencia adversaria el acceso a información sensible.

Los EEFI tienen que ver con intenciones propias, capacidades, y actividades que el adversario necesita conocer para planear y actuar de forma efectiva contra el cumplimiento de nuestra misión. Y dada la tendencia creciente al uso de las tecnologías de la información, los EEFI se van a encontrar cada vez más frecuentemente en sistemas de información tanto clasificados como sin clasificar.

Por lo tanto, el propósito de las OPSEC es reducir la vulnerabilidad propia hacia la explotación adversaria de información sensible. Y esto se realiza a través de un proceso sistemático para identificar, controlar y proteger dicha información.

El proceso OPSEC se lleva a cabo en cinco fases[26]:

- Identificación de la información sensible.

25 NATO STANDARDIZATION AGENCY «AJP-3.10 Allied Joint Doctrine for Information Operations, Ed A, ver 1.» Diciembre 2015, pág 1-14.

26 U.S. Joint Publication 3-13.3 «Operations Security» pág II-2.

- Análisis de las amenazas.
- Análisis de las vulnerabilidades.
- Valoración del riesgo.
- Aplicación de medidas de seguridad de las operaciones adecuadas.

Lógicamente, cuando se trata de información almacenada, procesada o trasmitida por un sistema de información y telecomunicaciones, de lo que se trata es de impedir el acceso a este conocimiento por actores no autorizados. Por lo tanto, juega aquí un papel preponderante la ciberdefensa.

A lo largo de los siguientes apartados, se realizará una breve descripción de las fases del proceso OPSEC adaptado a la protección de los EEFI en un AOCD. Dado que la identificación de los EEFI ya fue expuesta, se comenzará la exposición a partir de la segunda fase: el análisis de la amenaza.

Análisis de la amenaza

El desarrollo de esta fase consiste en el análisis de toda la información disponible que permita identificar los potenciales adversarios que podrían oponerse al cumplimiento de la misión.

Particularizado para un AOCD, se deben estudiar las amenazas que pudieran tener como propósito acceder a la información contenida en nuestros sistemas de información y telecomunicaciones.

Cuando existe amenaza de ciberataques, es necesario conocer qué tipo de tácticas, técnicas y procedimientos emplean los adversarios. De esta forma, se podrán planear medidas de seguridad adaptadas a las capacidades del adversario.

Según la doctrina nacional, es el Centro de Inteligencia de las Fuerzas Armadas, en el nivel operacional, el que tiene como cometido la elaboración y difusión de la valoración de la amenaza para cada una de las situaciones, áreas geográficas y operativas.[27]

Con objeto de que el análisis sirva posteriormente para aplicar la metodología de gestión del riesgo, se deberá estudiar:

27 ESTADO MAYOR DE LA DEFENSA. PDC «Doctrina Conjunta de Protección de la Fuerza». Septiembre 2014, pág 16. (publicación experimental).

- Capacidad de la amenaza. La que cada una tiene para acceder a la información almacenada, procesada o transmitida por nuestros sistemas de información y telecomunicaciones y que pueda afectar al cumplimiento de la misión.
- Intención de la amenaza. La que tiene para realizar actividades de obtención de información sobre nuestros CIS.
- Objetivos de la amenaza. Si el adversario no tiene intención de lograr sus objetivos en nuestros CIS, entonces no se espera que el adversario desencadene la amenaza.
- Probabilidad de la amenaza. Es la que tiene de explotar las vulnerabilidades que se detecten, basada sobre todo en el análisis histórico de circunstancias similares.

Así, si un actor hostil no tiene capacidad para explotar las vulnerabilidades de nuestros CIS, podremos decir que el riesgo es bajo.

Sin embargo, el análisis de la amenaza es complejo, especialmente cuando se trata de actores estatales, pues, aunque no dispongan de ciertas capacidades ciberespaciales, siempre cabe la posibilidad de que acaben subcontratándolas a actores no estatales.

En las «**tablas II, III y IV**» se pueden observar una posible valoración de la capacidad, intención y selección de objetivos por parte de un potencial adversario.

Tabla II

Valoración	Valores		Descripción
Muy alta	96-100	10	**Actores de amplio alcance**. Disponen de expertos y capacidades para llevar a cabo espectro completo de operaciones en el ciberespacio.
Alta	80-95	8	**Actores desarrolladores de programas**. Actores con amplio acceso a tecnologías de la información a través de la industria. Desarrollan programas para operar en el ciberespacio y poseen capacidades de espionaje tradicional.
Moderada	21-79	5	**Actores capaces**. Actores que poseen capacidades de espionaje tradicional y capacidades de desarrollar operaciones en el ciberespacio. No disponen de los recursos para de los actores desarrolladores de programas.
Baja	5-20	2	**Actores con capacidad de acceso remoto**. Pueden acceder a sistemas conectados a internet mediante el uso de herramientas disponibles de fuentes abiertas, pero no disponen de capacidad de espionaje tradicional.
Muy baja	0-4	0	**Actores independientes**. Acceso a expertos en hardware y software pero que no muestran evidencias de llevar a cabo operaciones en el ciberespacio o actividades de espionaje tradicional.

Tabla II: Valoración de las capacidades del adversario Fuente: Elaboración propia.

Tabla III

Valoración	Valores		Descripción
Muy alta	96-100	10	El adversario busca la obtención de los EEFI a través de la explotación de los sistemas de información propios.
Alta	80-95	8	El adversario trata de mantener su presencia en los sistemas de información propios para tratar de obtener los EEFI en el futuro.
Moderada	21-79	5	El adversario busca establecer una puerta de entrada en nuestros sistemas de información para tener acceso a los EEFI en un futuro.
Baja	5-20	2	El adversario busca activamente la obtención de los EEFI sin tener en cuenta los sistemas de detección de ciberataques propios.
Muy baja	0-4	0	El adversario trata de obtener acceso a nuestros sistemas de información sin tener en cuenta los sistemas de detección de ciberataques propios.

Tabla III: Valoración de la intención del adversario. (Fuente: elaboración propia).

Tabla IV

Valoración	Valores		Descripción
Muy alta	96-100	10	El adversario analiza la información obtenida a través de los reconocimientos y ciberataques con el objetivo de obtener acceso a los EEFI.
Alta	80-95	8	El adversario analiza la información obtenida a través de los reconocimientos con el objetivo de obtener acceso a los EEFI.
Moderada	21-79	5	El adversario analiza la información públicamente disponible para tratar de obtener información que pueda dar acceso a los EEFI.
Baja	5-20	2	El adversario usa la información públicamente disponible para centrarse en obtener información específica de alto valor y busca objetivos de oportunidad en ese rango.
Muy baja	0-4	0	El adversario podría no tener como objetivo la obtención de información de nuestros sistemas.

Tabla IV: Valoración de la selección de objetivos del adversario. (Fuente: elaboración propia).

Análisis de vulnerabilidades

Una vulnerabilidad es una debilidad en un sistema de información, procedimiento de seguridad del sistema, control interno o implementación que podría ser explotado por una amenaza[28].

La mayoría de las vulnerabilidades de los sistemas están asociadas con los controles de seguridad que, o bien no han sido implementados o aun siendo implementados, contienen alguna debilidad.

El propósito de esta fase es identificar vulnerabilidades en los sistemas de información y telecomunicaciones que podrían revelar información sensible y compararlas con las capacidades que tiene adversario, identificadas en la fase anterior.

Estas vulnerabilidades están generalmente asociadas con debilidades explotables que tienen que ver con deficiencias en el hardware, *software* o *firmware* de los sistemas de información o con los controles de seguridad empleados dentro de estos sistemas.

La severidad de una vulnerabilidad es una valoración de la importancia relativa que tendría su mitigación. Debido a la complejidad de la estructura CIS en una operación, el número de vulnerabilidades tiende a ser bastante grande y puede incrementarse en función de la complejidad del análisis.

Por lo tanto, es necesario clasificar las vulnerabilidades y destacar cuales son relevantes teniendo en cuenta las capacidades del adversario.

Una posible forma de hacerlo es a través de una escala de valoración de la severidad de las vulnerabilidades. En la «**tabla V**» se propone un posible modelo.

28 U.S. DEPARTMENT OF COMMERCE. *National Institute of Standards and Technology* «NIST 800-30 Guide for Conducting Risk Assessments». Septiembre 2012, pág 9.

Tabla V

Valoración	Valores		Descripción
Muy alta	96-100	10	La vulnerabilidad está expuesta y es explotable, y su explotación podría tener como consecuencia un impacto severo en nuestra misión. No se han implementado controles de seguridad apropiados y tampoco están planeados. Ninguna medida de seguridad puede ser identificada para poner remedio a la vulnerabilidad.
Alta	80-95	8	La vulnerabilidad es de alto interés, teniendo en cuenta la exposición de la vulnerabilidad y la facilidad de explotación y/o la severidad del impacto que podría resultar de su explotación. Están planeados controles de seguridad apropiados u otras medidas de mitigación, pero no implementados. Controles transitorios han sido puestos en marcha, pero son mínimamente efectivos.
Moderada	21-79	5	La vulnerabilidad es de interés moderado, teniendo en cuenta la exposición de la vulnerabilidad y la facilidad de explotación y/o la severidad del impacto que podría resultar de su explotación. Controles de seguridad apropiados u otras medidas de mitigación han sido parcialmente implementadas y hasta cierto punto efectivas.
Baja	5-20	2	La vulnerabilidad es de bajo interés, pero la efectividad de las medidas de mitigación podría ser mejoradas. Controles de seguridad apropiados u otras medidas de mitigación están totalmente implementadas y hasta cierto punto efectivas.
Muy baja	0-4	0	La vulnerabilidad no es de interés. Controles de seguridad apropiados u otras medidas de mitigación han sido totalmente implementadas, valoradas y efectivas.

Tabla V: Valoración de la severidad de las vulnerabilidades[29]

Adicionalmente a las vulnerabilidades descritas con anterioridad, es necesario considerar la exposición de los CIS. La exposición es una condición que afecta a la probabilidad de que una amenaza, una vez desencadenada, tenga como resultado un impacto adverso en las operaciones.

Así, el aislamiento de un sistema de información, sin conectividad a redes externas, disminuiría la probabilidad de exposición a un ciberataque a través de internet.

Las vulnerabilidades, incluidas aquellas atribuidas a la exposición, son parte de las condiciones de seguridad en las que opera un sistema de información y que pueden afectar a la probabilidad de ocurrencia de una amenaza.

29 U.S. DEPARTMENT OF COMMERCE. *National Institute of Standards and Technology* «NIST 800-30 Guide for Conducting Risk Assessments». Septiembre 2012, pág F-2.

Una posible valoración de la exposición se muestra en la «**tabla VI**».

Tabla VI

Valoración	Valores		Descripción
Muy alta	96-100	10	Se detectan en **todos** los sistemas de información que contienen datos que están relacionados con los EEFI.
Alta	80-95	8	Se detectan en **la mayoría** los sistemas de información que contienen datos que están relacionados con los EEFI.
Moderada	21-79	5	Se detectan en **muchos** sistemas de información que contienen datos que están relacionados con los EEFI.
Baja	5-20	2	Se detectan en **algunos** sistemas de información que contienen datos que están relacionados con los EEFI.
Muy baja	0-4	0	Se detectan en **algún** sistema de información que contienen datos que están relacionados con los EEFI.

Tabla VI: Valoración de la exposición. (Fuente: elaboración propia).

Valoración del riesgo

El objetivo de esta fase es la elaboración de una lista priorizada de riesgos que servirá para la posterior toma de decisiones.

La valoración del riesgo incluye generalmente los siguientes cometidos:

- Identificar los actores hostiles que son relevantes para la operación.
- Identificar las capacidades cibernéticas que poseen dichos actores.
- Identificar las vulnerabilidades propias que podrían ser explotadas por los adversarios a través de ciberataques.
- Determinar la probabilidad de que un adversario inicie un ciberataque para obtener información y la probabilidad de que sea exitoso.
- Determinar el impacto en operación producido por la explotación de vulnerabilidades realizado por el adversario.
- Determinar los riesgos en la seguridad de la información como combinación de probabilidad de explotación de vulnerabilidades por parte del actor hostil y el impacto de dicha explotación.

La valoración del riesgo se puede realizar en función de diferentes modelos. Cada uno de ellos tiene en cuenta diferentes factores de riesgo y las relaciones que tienen entre sí.

Los factores que se emplean en la presente monografía son las amenazas, las vulnerabilidades, la exposición, el impacto y la probabilidad de ocurrencia.[30]

Puesto que ya se han tratado con anterioridad las amenazas, vulnerabilidades y exposición, para completar la valoración del riesgo es necesario definir la probabilidad de ocurrencia y el impacto.

La probabilidad de ocurrencia

La probabilidad de ocurrencia es un factor de riesgo basado en el análisis de la probabilidad de que una amenaza sea capaz de explotar una vulnerabilidad dada. Para ello, se deben seguir un proceso constituido por tres fases, que determinará la probabilidad total de que se materialice una amenaza.

En primer lugar, se debe valorar la probabilidad de que una amenaza se materialice. Posteriormente, hay que valorar la probabilidad de que una amenaza, una vez iniciada, tenga como consecuencia un impacto adverso en las operaciones.

Por último, se debe valorar la probabilidad total como una combinación de probabilidad de ocurrencia y probabilidad de que resulte en impacto adverso.

La valoración de la probabilidad de desencadenamiento de una amenaza, se realiza teniendo en consideración las características de la amenaza, incluyendo capacidades, intención y selección de objetivos, ya descritas en el apartado 2.1.

En la «**tabla VII**» se expone una referencia para su valoración:

30 Existen otros modelos de valoración del riesgo, como el «SPE Risk Assesment Model», empleado en el ámbito de la Protección de la Fuerza en países como el Reino Unido y que usa la fórmula Riesgo= Impacto x Probabilidad x Exposición. A pesar de su simpleza, durante esta investigación se ha preferido usar el modelo contenido en la NIST 800-30 por considerarse más adaptado a riesgos en el ciberespacio.

Tabla VII

Valoración	Valores		Descripción
Muy alta	96-100	10	Se considera **prácticamente seguro** que el adversario desencadene la amenaza.
Alta	80-95	8	Se considera **altamente probable** que el adversario desencadene la amenaza.
Moderada	21-79	5	Se considera **probable** que el adversario desencadene la amenaza.
Baja	5-20	2	Se considera **improbable** que el adversario desencadene la amenaza.
Muy baja	0-4	0	Se considera **altamente improbable** que el adversario desencadene la amenaza.

Tabla VII: Valoración de la probabilidad de materialización de la amenaza[31]

Una vez valorada la probabilidad de materialización de la amenaza, se necesita determinar la probabilidad de que, una vez desencadenada, resulte en impacto adverso teniendo en cuenta las vulnerabilidades y exposición identificadas previamente.

Para establecer un valor para las diferentes probabilidades, se propone usar la escala expuesta en la **«tabla VIII»**.

Tabla VIII

Valoración	Valores		Descripción
Muy alta	96-100	10	Si la amenaza se materializa, es **prácticamente seguro** que se comprometa la confidencialidad de los EEFI.
Alta	80-95	8	Si la amenaza se materializa, es **altamente probable** que se comprometa la confidencialidad de los EEFI.
Moderada	21-79	5	Si la amenaza se materializa, es **probable** que tenga se comprometa la confidencialidad de los EEFI.
Baja	5-20	2	Si la amenaza se materializa, es **improbable** que tenga se comprometa la confidencialidad de los EEFI.
Muy baja	0-4	0	Si la amenaza se materializa, es **altamente improbable** que se comprometa la confidencialidad de los EEFI.

Tabla VIII: Valoración de la probabilidad de materialización de la amenaza. (Fuente: elaboración propia).

31 U.S. DEPARTMENT OF COMMERCE. *National Institute of Standards and Technology* «NIST 800-30 Guide for Conducting Risk Assessments». Septiembre 2012, pág G-2.

Las amenazas para las cuales no hay vulnerabilidades o exposición identificadas, tienen una muy baja probabilidad de tener impacto y, por lo tanto, de obtener acceso a los EEFI. Sin embargo, no deben descartarse para futuras valoraciones.

La probabilidad total de la amenaza es la combinación de la probabilidad de que sea desencadenada por el adversario y la probabilidad de que la materialización resulte en impacto adverso.

El empleo de reglas para combinar la probabilidad de los valores depende de la actitud de la organización hacia el riesgo, la tolerancia hacia la incertidumbre en diferentes factores de riesgo o la ponderación de los factores de riesgo.

Así, se podrían usar alguna de estas reglas[32]:

- Usar el mayor valor de las dos probabilidades.
- Usar el menor de los valores de las probabilidades.
- Considerar la probabilidad de iniciación/ocurrencia solo, asumiendo que, si la amenaza se inicia, resultarán en impacto adverso.
- Considerar la probabilidad del impacto solo, asumiendo que, si la amenaza pudiera resultar en impacto adverso, los adversarios desencadenaran la amenaza.
- Tomar una media ponderada de las probabilidades de los dos valores.

En el caso de optar por la última de las opciones, se propone la «**tabla IX**».

Tabla IX

Probabilidad de materialización de la amenaza	**Probabilidad de que una amenaza tenga un impacto adverso**				
	Muy baja	**Baja**	**Moderada**	**Alta**	**Muy Alta**
Muy alta	Moderada	Moderada	Alta	Muy alta	Muy alta
Alta	Baja	Moderada	Moderada	Alta	Muy alta
Moderada	Baja	Baja	Moderada	Moderada	Alta
Baja	Muy baja	Baja	Baja	Moderada	Moderada
Muy baja	Muy baja	Muy baja	Baja	Baja	Moderada

Tabla IX: Valoración de la probabilidad total de la amenaza. (Fuente: elaboración propia).

32 U.S. DEPARTMENT OF COMMERCE. *National Institute of Standards and Technology* «NIST 800-30 Guide for Conducting Risk Assessments». Septiembre 2012, pág 34.

El impacto

La medida del impacto se corresponde con el nivel de la magnitud del daño que puede provocar la materialización de una amenaza que resulta en un acceso no autorizado a un EEFI.

Este impacto debe estar referido a las consecuencias que tendría sobre el cumplimiento de la propia misión.

Para determinar la magnitud del impacto, es necesario considerar las características de las amenazas, las vulnerabilidades y exposición que han sido identificadas en el proceso.

La valoración del impacto puede implicar la identificación de componentes u objetivos potenciales de las amenazas. Esto incluye aquellos dispositivos donde se almacena la información, es decir, bases de datos, sistemas de información, aplicaciones, tecnologías de la información, enlaces de comunicaciones etc… que podrían verse afectados por las amenazas.

Una posible categorización del impacto es la que se puede observar en la **«tabla X»**.

Tabla X

Valoración	Valores		Descripción
Muy alto	96-100	10	La materialización de la amenaza podría tener consecuencias **múltiples y severas** sobre las operaciones.
Alto	80-95	8	La materialización de la amenaza podría tener consecuencias **severas** sobre las operaciones. Por ejemplo, podrían causar la pérdida de capacidades durante un periodo de tiempo a lo largo del cual se impida el cumplimiento de la misión.
Moderado	21-79	5	La materialización de la amenaza podría tener consecuencias **serias** sobre las operaciones. Por ejemplo, podrían causar una degradación significativa en las capacidades durante un periodo de tiempo en el que se puede cumplir la misión, pero con una efectividad fuertemente reducida.
Bajo	5-20	2	La materialización de la amenaza podría tener consecuencias **limitadas** sobre las operaciones. Por ejemplo, podrían causar una degradación significativa en las capacidades durante un periodo de tiempo en el que se puede cumplir la misión, pero con una efectividad reducida.
Muy bajo	0-4	0	La materialización de la amenaza podría tener consecuencias **insignificantes** sobre las operaciones.

Tabla X: Valoración del impacto causado por la materialización de la amenaza[33]

33 Basado en U.S. DEPARTMENT OF COMMERCE. U.S. DEPARTMENT OF COMMERCE.

Determinación del riesgo[34]

Llegados a este punto, tan sólo queda valorar el riesgo que procede de la materialización de amenazas contra la pérdida de confidencialidad de nuestros EEFI. Esto se calculará a través de una combinación de probabilidad e impacto.

El nivel de riesgo asociado con la materialización de una amenaza en el AOCD representa el grado en el cual una organización está amenazada.

Una posible matriz de valoración del riesgo puede observarse en la «**tabla XI**».

Tabla XI

Probabilidad de materialización de la amenaza y que resulte en impacto adverso	**Nivel de impacto**				
	Muy bajo	**Bajo**	**Moderado**	**Alto**	**Muy Alto**
Muy alta	Muy bajo	Bajo	Moderado	Alto	Muy alto
Alta	Muy bajo	Bajo	Moderado	Alto	Muy alto
Moderada	Muy bajo	Bajo	Moderado	Moderado	Alto
Baja	Muy bajo	Bajo	Bajo	Moderado	Moderado
Muy baja	Muy bajo	Muy bajo	Muy bajo	Bajo	Moderado

Tabla XI: Valoración del riesgo. (Fuente: elaboración propia).

Una vez obtenida la valoración del riesgo, es momento de ordenar la lista de posibles acciones del adversario en función su nivel de riesgo. A continuación, se deben priorizar los riesgos que den como resultado un mismo nivel o puntuación similar. Cada riesgo corresponde a una amenaza específica con un nivel de impacto determinado en el caso de que la amenaza se materialice.

En general, el nivel de riesgo no sobrepasa el nivel de impacto y la probabilidad puede servir para reducir el riesgo por debajo del nivel de impacto. Sin embargo, cuando se está tratando de gestionar un gran número de sistemas de información, no se sostiene que el impacto sea la frontera superior.

National Institute of Standards and Technology «NIST 800-30 Guide for Conducting Risk Assessments». Septiembre 2012, pág H-2.

34 En el ANEXO C se ilustra el modelo de valoración del riesgo que hemos seguido hasta ahora incluyendo los factores de riesgo claves y las relaciones entre ellos.

Para mostrarlo con un ejemplo, cuando se materializan múltiples riesgos, incluso cuando cada riesgo es moderado, el conjunto de esos riesgos de nivel moderado podría provocar un riesgo de nivel superior.

La respuesta al riesgo y la resiliencia

Tratamiento del riesgo

Una vez obtenida una valoración del riesgo, se puede responder a este de diferentes formas. Estas incluyen la aceptación del riesgo, la evitación, la mitigación, su transferencia o una combinación de las anteriores.

Las medidas de respuesta del riesgo dependen del tiempo y de la situación concreta. Por ejemplo, en una situación de emergencia, se podría aceptar el riesgo asociado con una conexión sin filtrar con un proveedor de servicios de comunicaciones externo por un tiempo limitado.

En este caso, se evitaría el riesgo cortando la conexión, se mitigaría en el corto plazo aplicando controles de seguridad para buscar *malware* o evidencias de accesos no autorizados y finalmente se mitigaría el riesgo en el largo plazo aplicando controles para el manejo de esa conexión de forma más segura.

La **aceptación del riesgo** es la respuesta apropiada cuando el riesgo identificado está dentro de la tolerancia de la organización. En función de la situación, se puede aceptar un riesgo valorado como bajo, moderado o alto. Por ejemplo, podría decidirse compartir información muy sensible con organizaciones que no tienen generalmente acceso a dicha información si esta es sensible al tiempo, como podrían ser acciones inminentes.

La **evitación del riesgo**, podría ser la respuesta apropiada cuando los riesgos identificados exceden la propia tolerancia al riesgo. El desarrollo de ciertos tipos de actividades o el empleo de ciertas tecnologías de la información pueden tener como resultado un riesgo inaceptable.

En esas situaciones, la evitación del riesgo incluye la puesta en marcha de acciones específicas para eliminar las actividades o las tecnologías que son base del riesgo. Por ejemplo, cuando se planea el empleo de conexiones de red entre dos dominios, se puede determinar a través de la valoración de riesgo que este es inaceptable.

Se podría evitar el riesgo a través de la eliminación de la conexión de red y emplear procesos de conexión manuales, a través de la transferencia de datos a través de dispositivos de almacenamiento secundarios.

La **transferencia del riesgo** traslada la responsabilidad del riesgo de un organismo a otro. Esto ocurre generalmente cuando un organismo estima que afrontar un riesgo requiere de expertos o recursos que son provistos de manera más eficiente por otro organismo. Esto podría darse cuando un Ejército considera que no tiene capacidad para reducir el riesgo en alguno de sus sistemas de información y solicita que este sea gestionado por otra entidad más especializada, como podría ser el Mando Conjunto de Ciberdefensa.

Por último, la mitigación del riesgo es la respuesta apropiada para aquella parte del riesgo que no puede ser aceptada, evitada, compartida o transferida. Por ejemplo, la mitigación del riesgo puede incluir políticas de uso de la red o dispositivos de seguridad y contramedidas más exigentes.

En este sentido, es ampliamente reconocido que el eslabón más débil de la cadena de seguridad en los sistemas de información es la persona. La escasa concienciación se manifiesta en comportamientos que, por desconocimiento, ponen en peligro la confidencialidad de información sensible, como puede ser el caso de la elaboración y tratamiento este tipo de información en sistemas no seguros.

En consecuencia, la puesta en marcha de planes de concienciación y formación en todo lo relativo a seguridad de la información en los CIS son siempre medidas de mitigación del riesgo que complementarán a otras medidas.

Es el caso de las medidas operativas, como el empleo la destrucción física y de la guerra electrónica o de las medidas técnicas, como la instalación de parches que limiten un ciberataque o el uso de cifradores para la protección de comunicaciones de voz, datos o video.

En cualquier caso, no hay que perder de vista que el planeamiento OPSEC es un proceso continuo, a lo largo de todas las fases de la operación.

La resiliencia y la mitigación de riesgos

Durante la presente investigación, se ha desarrollado el análisis de riesgos de un modo tradicional, centrado en el impacto y la probabilidad. Algunos autores, sin embargo[35], consideran que este enfoque no es apropiado para analizar los riesgos relacionados con

35 ENDRESEN, *Op. cit.* pág. 23.

ciberamenazas, puesto que el método tradicional requiere datos sobre un gran número de variables para poder estimar el riesgo.

Mientras que algunos datos pueden ser obtenidos de amenazas conocidas, basadas en ataques que ya han ocurrido antes en algún lugar, el gran ritmo con el que las capacidades cibernéticas se desarrollan hace que no haya datos suficientes sobre amenazas como para realizar una predicción fiable.

Por lo tanto, el enfoque tradicional de análisis de riesgo debe introducir el concepto de resiliencia a lo largo del proceso para tratar de afrontar aquellas amenazas no conocidas.

Para ello, es vital la comprensión de cómo nuestros sistemas críticos dependen del ciberespacio, las vulnerabilidades que esto provoca y la puesta en marcha de alternativas que proporcionen las capacidades y servicios necesarios.

La resiliencia consiste en reducir dependencias y vulnerabilidades. El grado de resiliencia en un sistema representa su habilidad para mantener sus capacidades críticas proporcionadas por el elemento atacado a través de mecanismos de prevención, detección, absorción y recuperación durante y después del ataque[36].

Por lo tanto, la mitigación de los riesgos debería ser considerada con respecto a las misiones, cometidos y responsabilidades de las unidades de ciberdefensa. Su capacidad de ser «resilientes» es una contribución crucial para transformar un riesgo cibernético inaceptable en uno que sea condicionalmente aceptable.

Conclusiones

Las tecnologías de las comunicaciones y de la información están cada vez más presentes en cualquier actividad humana, y las operaciones militares no son una excepción.

El ciberespacio se ha convertido en parte integrante del entorno operacional y de cada uno de los factores que lo definen. La capacidad de emplear el ciberespacio de forma segura a la vez que se deniega esta posibilidad al enemigo es una ventaja crucial para el éxito en las operaciones modernas.

Cada vez hay una mayor necesidad de intercambiar información entre las entidades de mando y control que participan en una operación.

36 Ibídem pág 23.

El paradigma de «necesidad de compartir» y nuevos conceptos como el *Federated Mission Networking* profundizarán en esta tendencia haciendo converger los sistemas de información y telecomunicaciones militares con el ciberespacio.

Por ello, se considera necesario delimitar la zona a defender dentro del dominio global del ciberespacio. En esa línea, se propone un concepto nuevo: el Área de Operaciones de Ciberdefensa (AOCD), entendida como *«conjunto de infraestructuras de tecnología de la información, las redes y los sistemas de información y telecomunicaciones que intervienen en el planeamiento y ejecución de una misión de nivel operacional y que es necesario proteger debido a la sensibilidad de la información que manejan.»*

Los sistemas de información y telecomunicaciones pertenecientes a un AOCD operarán en escenarios que estarán definidos por el tipo de actores que tengan capacidad de influir en el ciberespacio, sus capacidades cibernéticas y su intencionalidad.

En muchos casos, el AOCD será objeto de amenazas que buscarán explotar las vulnerabilidades que comprometan la confidencialidad de los elementos esenciales de información propia (EEFI) y poder así oponerse exitosamente al cumplimiento de la misión propia.

Dado que en el dominio cibernético no es posible la «seguridad total», es necesario concentrar los esfuerzos defensivos en la protección de aquella información que, de ser conocida por el adversario, pondría en peligro el cumplimiento de la misión.

Para ello, se propone la utilización del proceso de Seguridad de las Operaciones adaptado al dominio del ciberespacio en sus cinco fases: identificación de la información sensible, análisis de las amenazas, análisis de las vulnerabilidades, valoración del riesgo y aplicación de medidas de seguridad de las operaciones adecuadas.

En una primera fase, identificación de la información sensible, se deben distinguir los elementos esenciales de información propia en un proceso en el que deben estar involucradas todas las secciones del Estado Mayor. Según la doctrina OTAN, será la célula de Operaciones de Información la responsable de su identificación, principalmente a lo largo del análisis de la misión.

En esta fase hay que tener en cuenta que los propios CIS, o partes de ellos, pueden ser considerados EEFI. En consecuencia, se deben identificar los riesgos inherentes al conocimiento por parte del adversario de los activos que forman parte de nuestros sistemas. Para reducir el riesgo, se tendrán en cuenta los conceptos de segmentación, redundancia y puntos únicos de fallo.

Durante la segunda fase, análisis de la amenaza, se deben estudiar todos los potenciales adversarios que tengan capacidad de actuar en el ciberespacio, sus intenciones y sus objetivos. Para el desarrollo de la investigación, las capacidades que más interesan son aquellas que permiten la obtención de información sensible de nuestros CIS.

A lo largo de la tercera fase, análisis de vulnerabilidades, se deben identificar aquellas que puedan propiciar la revelación de información sensible. Estas vulnerabilidades hay que compararlas con las capacidades del adversario, puesto que, si no tienen capacidad para explotarlas, no serán motivo de preocupación.

A continuación, se debe valorar el riesgo conforme al modelo propuesto, en el que se tienen en cuenta las amenazas, las vulnerabilidades, la exposición, el impacto y la probabilidad de ocurrencia.

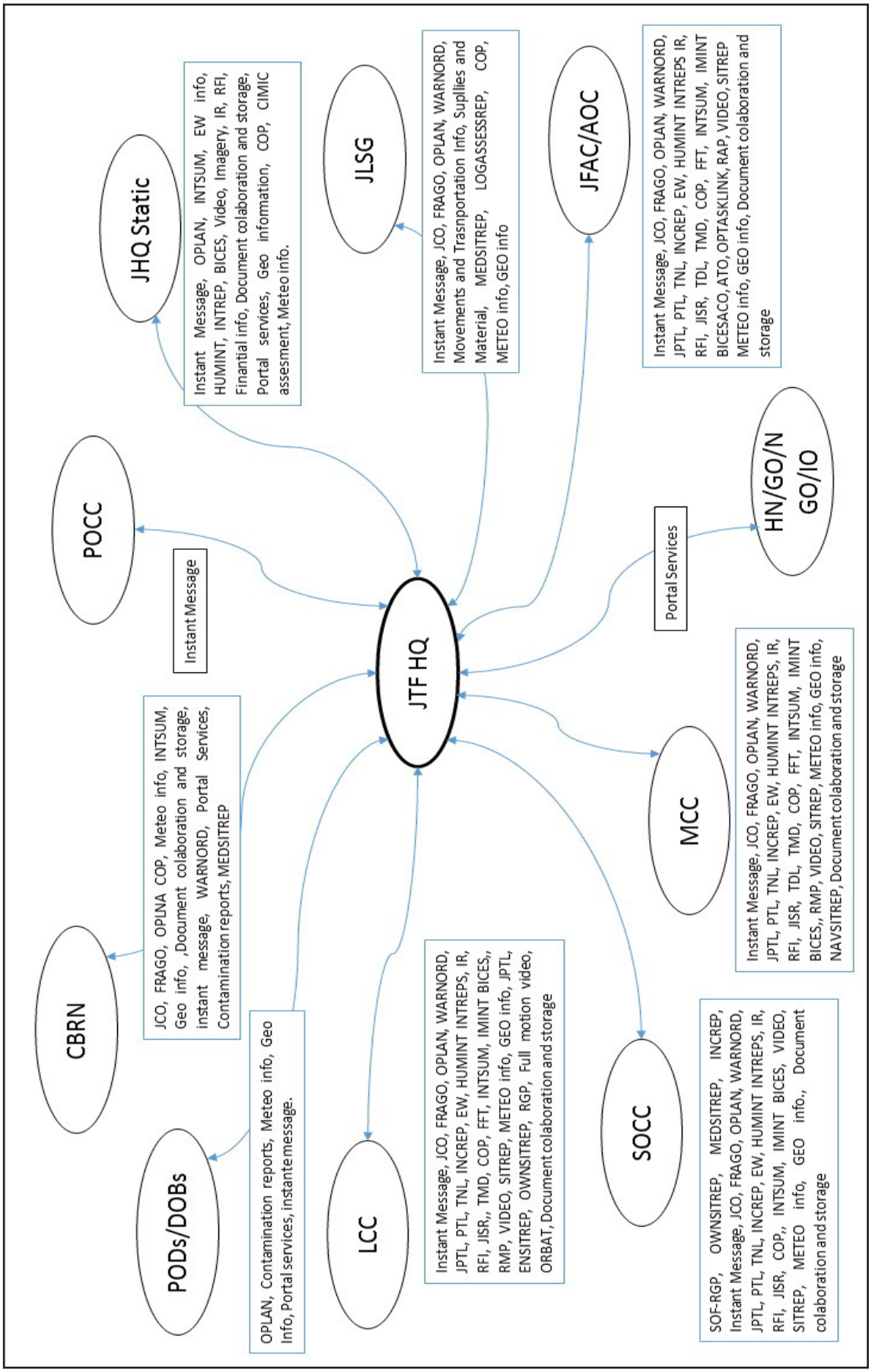
Una vez obtenida una valoración del riesgo, se debe elegir la respuesta adecuada según el tipo y nivel de riesgo. Esta podrá incluir la aceptación del riesgo, la evitación, la mitigación, su transferencia o una combinación de las anteriores.

El modelo de valoración del riesgo utilizado en la investigación, considerado como «tradicional», se centra en el impacto y la probabilidad. Su utilización en el dominio del ciberespacio tiene un inconveniente: en los casos en los que las amenazas aún no han sido utilizadas, no se puede contar con datos «históricos» que permitan su valoración.

Por ello y, debido a la rapidez con la que evoluciona el mundo cibernético, se considera necesario introducir el concepto de resiliencia en el AOCD como medida de mitigación de riesgos, al objeto de conseguir una respuesta más eficaz a las amenazas no registradas.

Anexo A

Diagrama de requisitos de intercambio de información


JHQ Static
Instant Message, OPLAN, INTSUM, EW info, HUMINT, INTREP, BICES, Video, Imagery, IR, RFI, Finantial info, Document colaboration and storage, Portal services, Geo information, COP, CIMIC assesment, Meteo info.
JLSG
Instant Message, JCO, FRAGO, OPLAN, WARNORD, Movements and Trasnportation Info, Supllies and Material, MEDSITREP, LOGASSESSREP, COP, METEO info, GEO info
JFAC/AOC
Instant Message, JCO, FRAGO, OPLAN, WARNORD, JPTL, PTL, TNL, INCREP, EW, HUMINT INTREPS IR, RFI, JISR, TDL, TMD, COP, FFT, INTSUM, IMINT BICESACO, ATO, OPTASKLINK, RAP, VIDEO, SITREP METEO info, GEO info, Document colaboration and storage
POCC
Instant Message
JTF HQ
Portal Services
HN/GO/NGO/IO
CBRN
JCO, FRAGO, OPLNA COP, Meteo info, INTSUM, Geo info, ,Document colaboration and storage, instant message, WARNORD, Portal Services, Contamination reports, MEDSITREP
MCC
Instant Message, JCO, FRAGO, OPLAN, WARNORD, JPTL, PTL, TNL, INCREP, EW, HUMINT INTREPS, IR, RFI, JISR, TDL, TMD, COP, FFT, INTSUM, IMINT BICES,, RMP, VIDEO, SITREP, METEO info, GEO info, NAVSITREP, Document colaboration and storage
PODs/DOBs
OPLAN, Contamination reports, Meteo info, Geo Info, Portal services, instante message.
LCC
Instant Message, JCO, FRAGO, OPLAN, WARNORD, JPTL, PTL, TNL, INCREP, EW, HUMINT INTREPS, IR, RFI, JISR,, TMD, COP, FFT, INTSUM, IMINT BICES,, RMP, VIDEO, SITREP, METEO info, GEO info, JPTL, ENSITREP, OWNSITREP, RGP, Full motion video, ORBAT, Document colaboration and storage
SOCC
SOF-RGP, OWNSITREP, MEDSITREP, INCREP, Instant Message, JCO, FRAGO, OPLAN, WARNORD, JPTL, PTL, TNL, INCREP, EW, HUMINT INTREPS, IR, RFI, JISR, COP,, INTSUM, IMINT BICES, VIDEO, SITREP, METEO info, GEO info., Document colaboration and storage

Anexo B

Posibles escenarios en un AOCD

Escenario A. Capacidad adversaria de reconocer y recolectar información

- En este escenario, el adversario cuenta con escasos recursos para realizar ciberataques contra nuestros sistemas de información y telecomunicaciones, pero aun así es capaz de realizar algunas de las siguientes actividades:
- Escanear/reconocer el perímetro de la red: uso de *software* comercial o libre para escanear el perímetro de nuestras redes informáticas con objeto de obtener un mejor conocimiento de nuestra infraestructura de tecnología de la información y mejorar su capacidad para ejecutar ataques exitosos.
- Realizar un reconocimiento del tráfico que transita a través de una red no protegida: capacidad de acceder a redes tanto alámbricas como inalámbricas usadas para trasmitir información con el objeto de identificar componentes, recursos y tipos de protección.

Llevar a cabo reconocimientos internos mediante el empleo de software maligno (*malware*): empleo *malware* instalado en el perímetro de nuestros sistemas para identificar objetivos de oportunidad.

Dado que estas actividades (escaneo, reconocimiento y observación) no cruzan el perímetro de nuestras redes, son difícilmente detectables por los sistemas de detección de intrusiones.

Escenario B. Capacidad adversaria confeccionar herramientas de ataque

- Este escenario incluiría alguna de las siguientes técnicas, tácticas o procedimientos:
- Confeccionar ataques «phishing»[1]: falsificación de las comunicaciones de una fuente fiable para adquirir información sensible como usuarios ycontraseñas.
- Confeccionar sitios web falsos: creación de duplicados de sitios web legítimos. Cuando un usuario de nuestra organización visita el sitio falso, se puede obtener información y provocar la descarga de *malware*.
- Confeccionar certificados falsos: el adversario falsifica una autoridad de certificación, de forma que el *malware* o la conexión aparezca como legítima.
- Crear u operar una organización falsa que introduzca componentes falsificados en la cadena de aprovisionamiento: creación de una empresa falsa que pueda inyectar componentes corruptos en los sistemas de información.

Escenario C. Capacidad adversaria de distribuir, insertar o instalar malware

- Continuando con el orden creciente en cuanto a capacidad del adversario, en este escenario se podrían encontrar alguna de las siguientes capacidades:
- Distribuir malware en el interior de los sistemas de información propios: empleo de los mecanismos de distribución comunes (p. ej., correo electrónico) para instalar/insertar *malware* en los sistemas de información.
- Distribuir *malware* dirigido al control de los sistemas internos y a la exfiltración de datos: instalación de malware que ha sido designado para tomar el control de los sistemas de información propios, identificar información sensible, exfiltrar la información y ocultar estas acciones.

Distribución de malware a través de dispositivos extraíbles: colocación de dispositivos extraíbles (p. ej., memorias portátiles) con malware en su interior en lugares externos al perímetro de los sistemas pero donde los miembros de la organización pueden encontrarlos y usarlos en los sistemas de información.

1 El «phishing» consiste en el empleo de mensajes de correo electrónico que aparentemente provienen de fuentes fiables con la intención de obtener datos confidenciales del usuario de manera fraudulenta (fuente: www.pandasecurity.com).

Escenario D. Capacidad adversaria de explotación

Este escenario y los que siguen, implican la capacidad de acceso por parte del adversario a potenciales EEFI alojados en nuestros sistemas de información mediante el empleo de capacidades avanzadas. Estas incluyen:

- Explotar sistemas de información conectados a internet o defectuosamente configurados: acceso a través de internet a sistemas de información que no están autorizados a conectarse a internet o que no cumplen con los requisitos de configuración establecidos.
- Explotar vulnerabilidades conocidas en sistemas móviles (ordenadores portátiles, teléfonos inteligentes, etc...): obtención de ventaja a través del hecho que sistemas de información transportables están fuera de la protección física y lógica de los centros autorizados para su manejo.
- Explotar vulnerabilidades usando ataques *zero-day*[2]: empleo de ataques que explotan las hasta el momento desconocidas vulnerabilidades del sistema.

Comprometer los sistemas de información, para facilitar la exfiltración de información: implantación de *malware* en los sistemas de información, de forma que el *malware* puede identificar información crítica y exfiltrarla.

Escenario E. Capacidad adversaria de conducir un ataque y lograr resultados

- Conducir ataques que intercepten comunicaciones: obtención de la ventaja que proporciona las comunicaciones que no están encriptadas o que usan una débil cifra y acceso a la información transmitida por dichos canales.
- Conducir ataques de fuerza bruta para acceder a los sistemas: acceso a los sistemas de información a través de la obtención de contraseñas mediante el empleo de herramientas de forzado de contraseñas.
- Obtener información sensible a través de la exfiltración: el adversario dirige el *malware* hacia los sistemas de información propios para localizar y, de manera oculta, transmitir información sensible.

2 Se denomina 'ataque *Zero Day*' a cualquiera lanzado aprovechando la ventana de oportunidad producida por vulnerabilidades recién descubiertas, antes de que los proveedores de seguridad hayan sido capaces de reparar la vulnerabilidad (fuente: www.pandasecurity.com).

Obtener información sensible de sistemas de información públicamente accesibles: escaneo de la información en los servidores públicamente accesibles con la intención de encontrar información sensible.

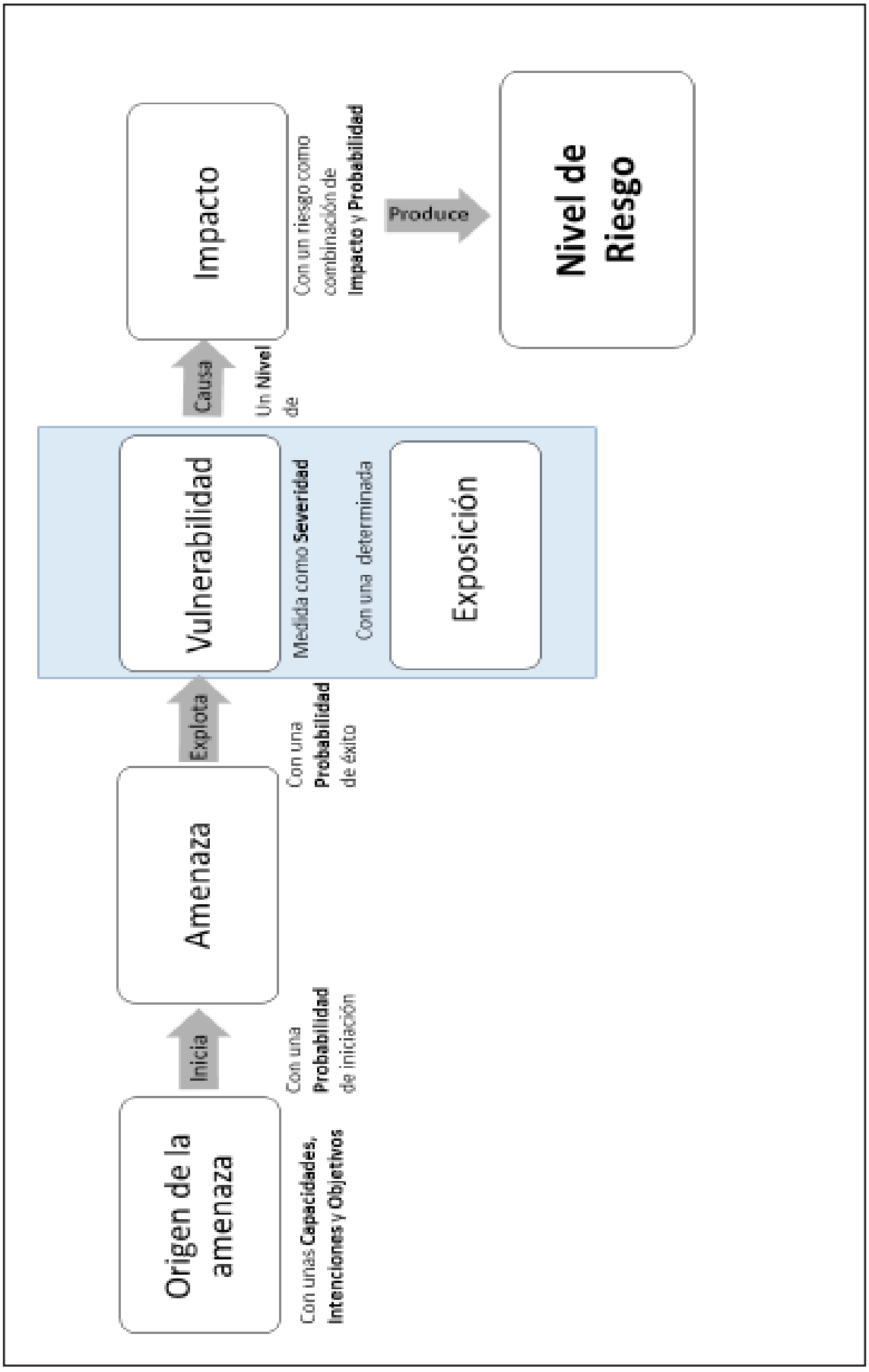
Escenario F. Capacidad adversaria para mantener la presencia y coordinar una campaña

- Confundir al adversario y adaptar los ciberataques: inhibición de las medidas de detección de intrusiones propias y adaptación del comportamiento adversario a las medidas de seguridad puestas en práctica.
- Coordinar una campaña que combine ataques internos y externos a lo largo de múltiples sistemas y tecnologías de información: combinación de ataques que requieren presencia física dentro de las instalaciones propias y métodos cibernéticos para conseguir el éxito.
- Coordinar una campaña que extienda los ataques a lo largo de los sistemas propios: empleo del acceso en un sistema para extender el control a otros sistemas.

Coordinar una campaña de ciberataques continuos, adaptativos y cambiantes basados en la observación detallada: realización de ciberataques en continuo cambio en respuesta a la vigilancia y medidas de seguridad propias.

Anexo C

Modelo de determinación del riesgo


Origen de la amenaza
Con unas Capacidades, Intenciones y Objetivos
Inicia
Con una Probabilidad de iniciación
Amenaza
Explota
Con una Probabilidad de éxito
Vulnerabilidad
Medida como Severidad
Con una determinada
Exposición
Causa
Un Nivel de
Impacto
Con un riesgo como combinación de Impacto y Probabilidad
Produce
Nivel de Riesgo


ESCUELA SUPERIOR DE LAS FUERZAS ARMADAS
Scientia atque Excellentia