Taxonomía de ciberejercicios

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

Este estudio ha sido elaborado con la coordinación y participación de Elena García Díez, Daniel Fírvida Pereira, Marco A. Lozano Merino, Héctor R. Suárez y Darío Beneitez Juan.

Marzo 2015

INDICE

1 INTRODUCCIÓN

Aunque se considera a John Dewey como el motor intelectual de la simulación a través de su obra "Education and Experience", (1938. New York, Collier), en la que argumentaba en contra del exceso de teoría[1], la idea de diseñar ambientes simulados para la enseñanza seguía siendo una novedad a finales de los años 60, pues se consideraba ésta como un proceso de aprendizaje establecido básicamente entre un educador capaz de transmitir conocimiento a los alumnos sobre un tema en particular, mediante la utilización de los medios aceptados (libros, conferencias, etc.).

Sin embargo, en esta década de los años 60 ya se puede mencionar el Ejercicio REFORGE (vuelta a Alemania), concebido por primera vez en 1967 por la Organización del Tratado del Atlántico Norte (OTAN) y realizado anualmente durante la Guerra Fría. Su objetivo era comprobar la capacidad de desplegar rápidamente fuerzas en Alemania Occidental en el caso de un conflicto con el Pacto de Varsovia.

A partir de los años 80, la simulación cobra cada vez más importancia como un medio de formación, y se puede decir que constituye una herramienta que ofrece la posibilidad de llevar a cabo de forma segura y controlada, una práctica análoga a la que se realizaría en la realidad ante las situaciones planteadas durante su ejecución.

Trasladado al mundo cibernético, podemos afirmar que un ciberejercicio es una herramienta que permite evaluar el estado de preparación de los participantes frente a crisis de origen cibernético, facilitando además lecciones aprendidas y recomendaciones para el futuro: aspectos de mejora frente un ataque cibernético, para el aumento de la cooperación y la coordinación dentro de los sectores involucrados, para la identificación de interdependencias, para la mejora de la concienciación y la formación, etc.

Aunque inicialmente, entre 2002 y 2004 el número de ciberejercicios realizados anualmente fue reducido, en los últimos años su celebración ha crecido considerablemente por alcance, ámbito geográfico, número de sectores involucrados y por perfil de participación.

Como ejemplo, en el capítulo 3 del presente documento se recopilan aquellos ciberejercicios realizados y que se han identificado atendiendo a la metodología empleada para el presente proyecto.

Su clasificación permitiría un mayor conocimiento del estado actual de los mismos y constituiría una herramienta para comprender y planificar las realizaciones de los mismos, tanto en el sector público como en el privado.

Por ello, en el presente documento, a partir de la información recopilada, se propone el esquema taxonómico o clasificatorio que se describe en el capítulo 4. Dicho esquema se

[1] http://www.labsag.co.uk/es/index.php/simuladores-de-negocios/historia-y-eficacia-de-la-simulacion/

corresponde con una taxonomía que se aplica en el capítulo 5 del presente documento a los ciberejercicios que se han considerado más relevantes.

1.1 ACRÓNIMOS

Acrónimos	
APCERT	Asia Pacific Computer Emergency Response Team
APEC	Asia-Pacific Economic Cooperation
CERT	Computer Emergency Response Team
EGC	European Government CERTs
ENISA	European Network and Information Security Agency
SOP	Standard Operating Procedure
TIC	Tecnologías de la Información y las Comunicaciones
OTAN	Organización del Tratado del Atlántico Norte

Tabla 1. Acrónimos

2 METODOLOGÍA DE TRABAJO

El objetivo de este documento es proponer una taxonomía de ciberejercicios y aplicarla a los que se han sido considerados más relevantes, con el fin de que constituya una herramienta de utilidad al servicio de la comunidad nacional e internacional de la ciberseguridad, proporcionando un mayor conocimiento los ciberejercicios existentes, y facilitando la planificación de futuras ediciones.

Se entiende por taxonomía una clasificación u ordenación de cosas en grupos que tengan unas características comunes. Teniendo en cuenta esta definición, la aplicación de una taxonomía de ciberejercicios permitirá obtener una caracterización de los mismos, y facilitará la identificación de lagunas actuales en su ejecución, a través del análisis de la aplicación de la taxonomía a los ciberejercicios considerados más relevantes.

Para conseguir este objetivo, se ha llevado a cabo un proceso que comienza con la obtención y el análisis de la información pública disponible sobre los distintos ciberejercicios que se han llevado a cabo hasta la fecha. El término ciberejercicio se utiliza en este documento para referirse a cualquier celebración o edición en el tiempo.

Por ejemplo, si se han celebrado varios ciberejercicios en distintos años bajo la denominación de "*Cyber Storm*", se considera un ciberejercicio distinto cada celebración.

Una vez obtenida y analizada la información, se ha elaborado una propuesta de taxonomía para los ciberejercicios identificados, y una posterior aplicación de la misma a aquellos que se han considerado más relevantes de acuerdo a un criterio previamente definido. La siguiente figura resume la metodología utilizada:

Figura 1. Metodología

En la primera fase de obtención de la información, se ha tratado de recopilar la mayor cantidad posible de información pública sobre los ciberejercicios existentes. Para ello, se han utilizado diversas fuentes, como la Agenda Digital para Europa, la Agencia Europea para la Seguridad de la Información, *European Union Agency for Network and Information Security* (ENISA) y la investigación online realizada hasta el 5 de septiembre de 2014 sobre todas las referencias de páginas web del presente documento.

Tras analizar la información recopilada, se han definido un conjunto de métricas e indicadores. Los resultados de estas métricas se han escrutado con el objetivo de establecer un perfilado de los ciberejercicios que presente distintos perfiles o características acerca de la ejecución de los mismos, y facilite la posterior definición de la taxonomía. Además, se ha valorado cómo de completa es la información recopilada, con el objetivo de tener presente que los resultados del análisis estarán condicionados por la información que ha sido posible recopilar sobre los mismos.

A partir del análisis y perfilado de los distintos ciberejercicios, y tomando como referencia los trabajos realizados por organizaciones de distinto ámbito geográfico relacionados con la tipificación de los mismos, se ha desarrollado una propuesta de taxonomía de ciberejercicios, con el fin de que pueda ser utilizada tanto por el sector público como por el sector privado para la planificación y mejora de ciberejercicios en el futuro.

Finalmente, se ha aplicado dicha taxonomía a los ciberejercicios que se han considerado más relevantes tras implementar las métricas, con el objetivo de mostrar la utilidad de la misma, y obtener conclusiones que puedan servir para profundizar en el conocimiento del estado actual de los mismos, y favorecer la planificación de nuevos ciberejercicios.

3 IDENTIFICACIÓN Y ANÁLISIS DE CIBEREJERCICIOS

A continuación se presenta la información recopilada sobre los diferentes ciberejercicios identificados a partir de diversas fuentes de información, que incluyen la implementación de la Agenda Digital para Europa, ENISA, y la investigación online.

La siguiente figura presenta los aspectos de la metodología de trabajo que se desarrollan a lo largo de este apartado:

Figura 2. Metodología para la obtención de información y el análisis de ciberejercicios

En primer lugar, se describe cómo ha sido el proceso de obtención de información pública, y qué fuentes se han utilizado para recopilarla.

Dado que no siempre se dispone de una información completa sobre los ciberejercicios, a continuación se presenta el grado de detalle de la información disponible sobre cada uno de ellos. El objetivo de valorar este aspecto es poner de manifiesto que los resultados del estudio podrían estar condicionados por la información pública que ha sido posible recopilar sobre los ciberejercicios. Así mismo, constituirá un criterio para la selección de los más relevantes, en el sentido de que aquellos para los que se disponga de más información, serán candidatos para la aplicación de la taxonomía.

3.1 OBTENCIÓN DE INFORMACIÓN

La primera fuente de información que se ha empleado ha sido la Agenda Digital para Europa[2]. Para su implementación en los estados miembros, la acción 39[3] que se encuentra dentro del pilar de "confianza y seguridad", está relacionada con la participación de los Estados en ciberejercicios y la planificación de futuras participaciones.

La información sobre la citada implementación se encuentra publicada en una página web con datos que se actualizan, tanto por los representantes de los estados miembros (usuarios registrados), como por cualquier persona que quiera aportar información relevante a través un formulario online. Gracias a dicha información, ha sido posible establecer las iniciativas abordadas por los países europeos en relación a los ciberejercicios que han realizado, tanto a nivel nacional como internacional.

Otra fuente importante de información ha sido ENISA[4]. Ésta publicó un documento en 2012[5], que contiene un catálogo de ciberejercicios realizados entre los años 2002 y 2012. Para ello llevaron a cabo dos tipos de actividades: por un lado recopilaron información durante 6 meses sobre los ciberejercicios, tanto en la literatura como en fuentes online, y por otro, realizaron una encuesta sobre los distintos ciberejercicios realizados, con el objeto de recabar información a través de los contactos de la propia agencia.

Cabe resaltar que la propia ENISA indica que no puede confirmar que la información obtenida sea completa y actualizada. Por este motivo, en el presente trabajo se ha realizado una nueva búsqueda individualizada de los ciberejercicios tratados previamente por la Agencia, identificando y actualizando las ediciones, en un intento de completar la información reportada previamente en su informe.

Además, con el objetivo de facilitar la armonización de la clasificación de los ciberejercicios, aparte de haber considerado los campos utilizados previamente por ENISA en la recopilación de información sobre los mismos, se han tenido en cuenta las clasificaciones realizadas por el grupo de trabajo de telecomunicaciones e información de la cooperación económica Asia-Pacífico, *Asia-Pacific Economic Cooperation* (APEC)[6].

---

[2] http://ec.europa.eu/digital-agenda/
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:ES:PDF

[3] http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-39-member-states-carry-out-cyber-attack-simulations

[4] http://www.enisa.europa.eu/

[5] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012/at_download/fullReport

[6] http://www.apec.org/

Por último, en lo que respecta a la obtención de información, se ha llevado a cabo un trabajo de investigación en diversas fuentes online, que ha permitido completar y actualizar el catálogo de los ciberejercicios realizados en el periodo 2012-2014, priorizando tanto los nuevos ciberejercicios, como aquellos otros que introducen elementos diferenciadores respecto a los identificados previamente, como pueden ser su enfoque, o la participación de nuevos sectores en los mismos.

3.2 INFORMACIÓN DISPONIBLE

La información que está disponible y se ha recopilado acerca de cada ciberejercicio presenta distintos grados de detalle. Por ejemplo, en el informe realizado por ENISA que se ha usado como referencia, prevalece la identificación de la totalidad de los ciberejercicios, sobre el grado de detalle de cada uno de ellos.

Otro aspecto importante a considerar, es que los organizadores de los ciberejercicios no siempre proporcionan la totalidad de la información sobre los mismos, tratándola en algunos casos como información sensible, no accesible públicamente.

Teniendo esto en cuenta, se ha valorado la información disponible sobre cada ciberejercicio, con el objetivo de poner de manifiesto que los resultados que se han obtenido están condicionados por la información que ha sido posible recopilar sobre los mismos.

Para realizar esta valoración, se han seguido los siguientes criterios sobre la completitud de la información:

- **Alta**: cuando la cantidad y calidad de la información recopilada se considera suficientemente completa, precisa y actualizada con los últimos ciberejercicios.
- **Media**: cuando la información recopilada está actualizada, pero no se considera con la calidad o cantidad suficiente para disponer de una visión completa del ciberejercicio.
- **Baja**: cuando se considera que la información recopilada no está actualizada, o bien se dispone de muy poca información.

La siguiente tabla resume la valoración de la completitud de la información que se ha podido recopilar para cada grupo de ciberejercicios identificado, entendiendo por grupo de ciberejercicios aquellos que tienen la misma denominación (por ejemplo Cyber Storm), independientemente del número de ediciones celebradas a lo largo del tiempo.

EJERCICIO	COMPLETITUD DE LA INFORMACIÓN
BLUE CASCADES	Media
CYBER STORM	Alta
GRIDEX	Alta
ASEAN CERT INCIDENT DRILL	Media

EJERCICIO	COMPLETITUD DE LA INFORMACIÓN
APCERT DRILL	Media
ITU IMPACT	Media
BALTIC CYBER SHIELD CYBER DEFENCE EXERCISE	Alta
LOCKED SHIELDS	Alta
PHOENIX	Media
CYBER ENDEAVOR	Media
CYBER CRISIS MANAGEMENT	Baja
CYBER COALITION	Baja
CYBERATLANTIC	Baja
CYBEREUROPE	Media
EUROCYBEX	Alta
EUROSOPEX	Baja
CYBER-EX	Media
PSCIC	Media
EJERCICIO DE CIBERDEFENSA	Baja
CYDER	Media
FIRST CYBERSECURITY WAR GAMES	Baja
SHIFT-CONTROL EXERCISE	Baja
PANOPTIS	Media
PIRANET	Baja
NATIONAL CYBER SECURITY EXERCISE	Alta
LÜKEX	Alta
BELGOCYBEX	Baja
CYBER ITALY	Baja
EVENTIDE	Baja
CYBER DEFENSE EXERCISE	Alta
OPERATION KILL SWITCH	Baja
NATIONAL LEVEL EXERCISE	Media
CYBER CHALLENGE	Media
COLLEGIATE CYBER DEFENSE COMPETITION	Media
QUANTUM DAWN	Media
CYBER AND OPERATIONAL RESILIENCE	Media
CYBER ATTACK PAYMENT PROCESSES	Media
CYBER GUARD	Baja
CYBERRX	Alta
ENRIC	Baja
GESTIÓN DE CRISIS DE CIBERSEGURIDAD	Baja
WAKING SHARK	Media

EJERCICIO	COMPLETITUD DE LA INFORMACIÓN
WHITE NOISE	Media
COMEX	Baja
SLOVAK INFORMATION SECURITY EXERCISE	Media
POST AND TELECOM AGENCY	Media
TELÖ	Media
TIETO	Baja
PLANSPIEL	Media
GAILLEAN	Baja
ECS	Baja
CYBER FEVER	Baja
CYBERWINTER	Media

Tabla 2. Completitud de la información recopilada por ciberejercicio

3.3 MÉTRICAS

El objetivo principal de definir métricas es realizar la evaluación y seguimiento del estado de seguridad, con el objetivo de emprender acciones de mejora.

Adicionalmente podemos definir indicadores, que son el resultado de aplicar un modelo analítico a una o más métricas, en relación con unos criterios objetivo. Si el criterio objetivo se define, por ejemplo, como el 100%, el indicador correspondiente nos dirá cuánto nos estamos aproximando a este valor objetivo.

A continuación se han identificado una serie de métricas con el objetivo de perfilar los ciberejercicios identificados y extraer conclusiones.

Se ha considerado, tanto las métricas por ciberejercicio, como métricas globales. Cada una lleva asociada su indicador correspondiente, que es el resultado de comparar dicha métrica con un valor objetivo, convirtiendo la métrica obtenida en información útil para realizar el perfilado de ciberejercicios.

Las siguientes tablas recogen las métricas que se han considerado, así como su indicador asociado.

MÉTRICAS POR CIBEREJERCICIO	INDICADOR
Nº de países involucrados/ciberejercicio	Participación de países en los ciberejercicios
Nº de países europeos involucrados/ciberejercicio	Participación europea en los ciberejercicios
Nº de entidades u organizaciones involucradas/ciberejercicio	Participación de entidades en los ciberejercicios

Nº de sectores verticales involucrados/ciberejercicio	Involucración de los distintos sectores verticales en los ciberejercicios

Tabla 3. Métricas por ciberejercicio e indicadores asociados

MÉTRICAS GLOBALES	INDICADOR
Nº de ciberejercicios internacionales en los que han participado países de la UR	Participación europea en los ciberejercicios internacionales (fuera de la UE)
Nº de ciberejercicios en los que ha participado España	Participación de España en los ciberejercicios
Nº de ciberejercicios internacionales en los que ha participado España	Participación de España en los ciberejercicios internacionales
Nº de ciberejercicios que afectan al sector público	Participación del sector público en los ciberejercicios
Nº de ciberejercicios que afectan al sector privado	Participación del sector privado en los ciberejercicios
Nº de ediciones celebradas/año	Evolución temporal de las ediciones de ciberejercicios
Nº de ciberejercicios *tabletop*	Escenarios de desarrollo de los ciberejercicios
Nº de ciberejercicios basados en escala real	
Nº de ciberejercicios que cubren todas las fases del incidente	Alcance de los ciberejercicios
Nº de ciberejercicios que cubren la fase previa a la ocurrencia del incidente	
Nº de ciberejercicios que cubren la fase durante la ocurrencia del incidente	
Nº de ciberejercicios que cubren la fase posterior al incidente	
Nº de familias de ciberejercicios que sólo se han llevado a cabo una vez	Continuidad de las familias de ciberejercicios en el tiempo
Nº de familias de ciberejercicios que se han llevado a cabo más de una vez, de manera regular	
Nº de ciberejercicios incluidos en la implementación de la Agenda Digital para Europa	Inclusión de ciberejercicios en la implementación de la Agenda Digital para Europa

Tabla 4. Métricas globales e indicadores asociados

3.4 PERFILADO DE CIBEREJERCICIOS

Tras aplicar las métricas anteriores a la información recopilada sobre los ciberejercicios, se han obtenido unos resultados que permiten elaborar un perfilado de los mismos según se detalla a continuación.

3.4.1 Participación de países y entidades en los ciberejercicios

Refleja el número de países y entidades/organizaciones participantes en los ciberejercicios, a nivel global, internacional, y nacional.

Este aspecto trata de poner de relieve la colaboración entre las naciones.

Entendemos por nivel global el número total de ciberejercicios que se han llevado a cabo; por nivel internacional, los ciberejercicios que implican a más de un país; y por nivel nacional, los ciberejercicios organizados a nivel de un único país.

- Países participantes en los ciberejercicios

Se ha analizado el número de países participantes en los ciberejercicios, diferenciando aquellos en los que sólo participa un país, frente aquellos en los que participan hasta 20 o más países.

Como se puede observar en la gráfica, la mayoría de los ciberejercicios se han realizado a nivel nacional (73%), frente a los ciberejercicios internacionales (27%). Esto se debe principalmente al grado de madurez de los ciberejercicios a lo largo del tiempo, de modo que las primeras celebraciones se realizan dentro de una nación, y no se involucran a más naciones hasta que no se alcanza determinado grado de madurez.

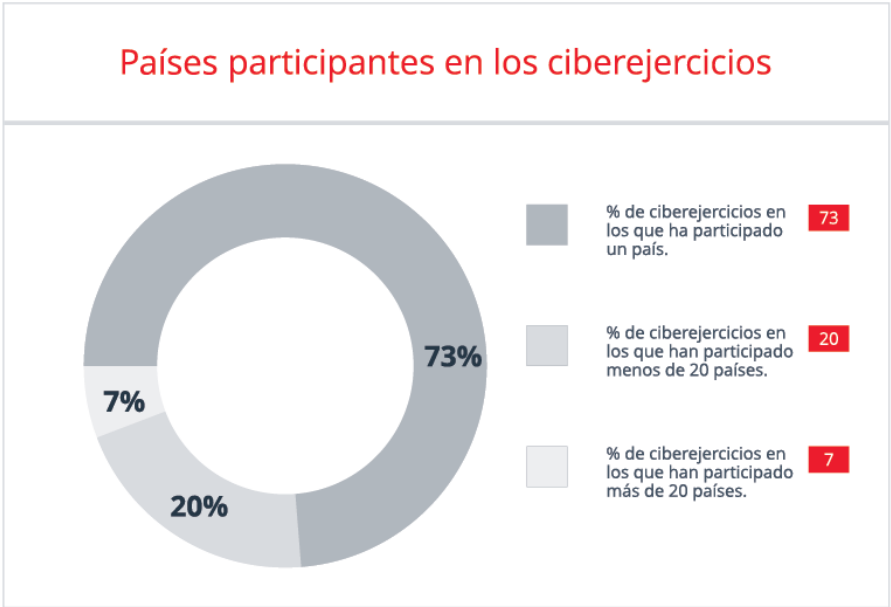

Figura 3. Países participantes en los ciberejercicios

- Países de la UE participantes en los ciberejercicios

En este caso se analiza la participación de países de la UE en el conjunto de todos los ciberejercicios, y como puede observarse en el gráfico, se concluye que los países de la UE han participado en más de la mitad de todos los ejercicios identificados.

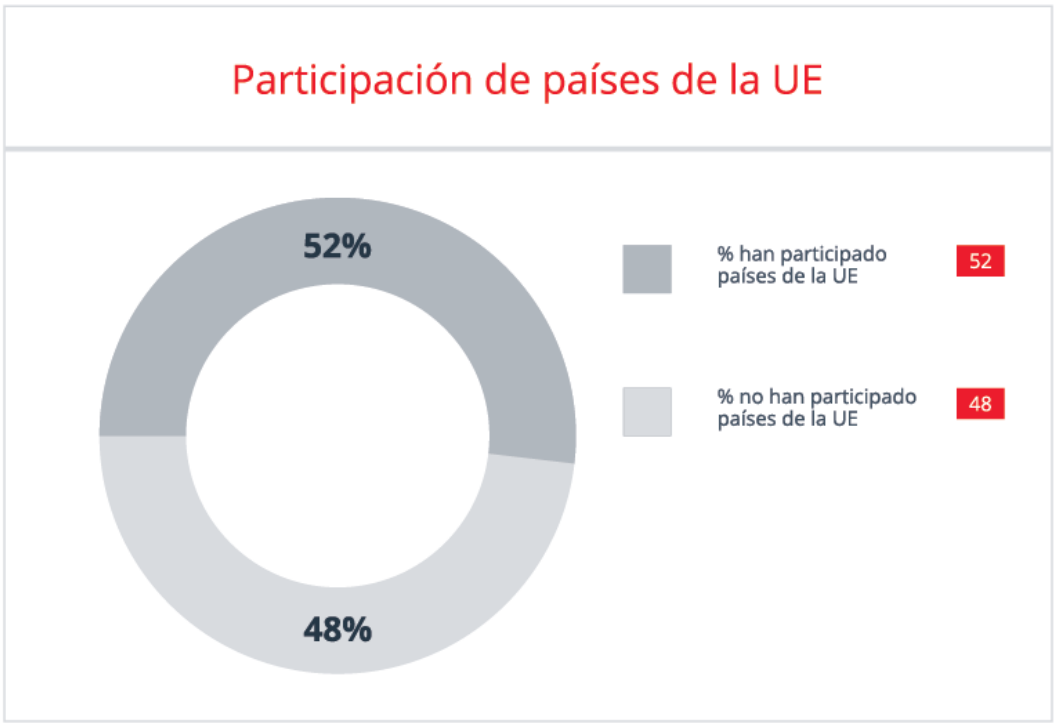

Figura 4. Países de la UE participantes en los ciberejercicios

Se ha considerado de interés valorar la participación de los estados miembros de la UE en los ciberejercicios organizados a nivel internacional, entendiéndose por éstos como aquellos que involucran a más de una nación.

El resultado obtenido es que los países de la UE han participado en casi la mitad de los ciberejercicios de nivel internacional analizados. Esto indica una participación activa de los países de la UE en el ámbito internacional.

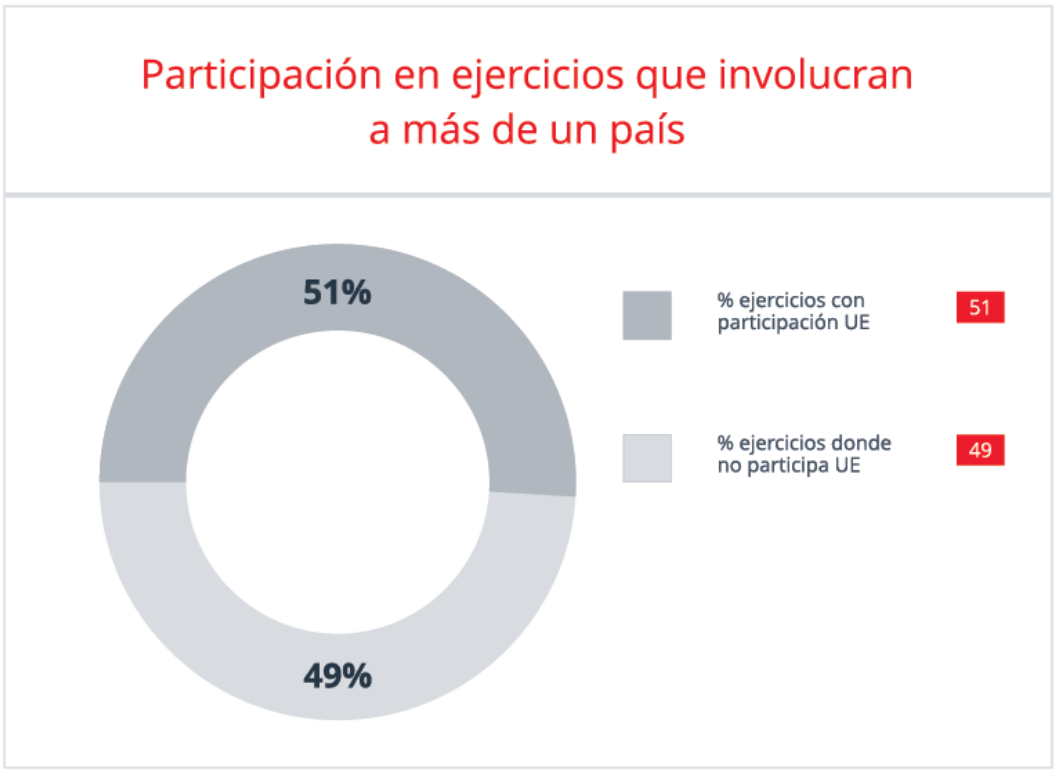

Figura 5. Países de la UE participantes en los ciberejercicios internacionales

Una vez hemos analizado el porcentaje de ciberejercicios en los que han participado estados miembros de la UE, se considera interesante valorar cuántos ciberejercicios internacionales han contado con una alta participación de dichos estados miembros.

Para ello, la siguiente gráfica presenta el porcentaje de ciberejercicios internacionales que han contado con la participación conjunta de varios estados miembros de la UE, diferenciando entre aquellos ciberejercicios en los que participan conjuntamente hasta 20 estados miembros de la UE, y aquellos en los que esta participación supera los 20 países. La conclusión que obtenemos es que alrededor de un 16% de ciberejercicios internacionales han contado con la participación conjunta de hasta 20 países de la UE, y más de 20 países de la UE han participado conjuntamente solamente en un 7% de ciberejercicios organizados a nivel internacional.

Este análisis pone de manifiesto la alta participación de los países Europeos en ciberejercicios de carácter internacional, estando alineado con la tendencia de que los ciberejercicios incrementen su grado de internacionalización, buscando incrementar el número de países participantes.

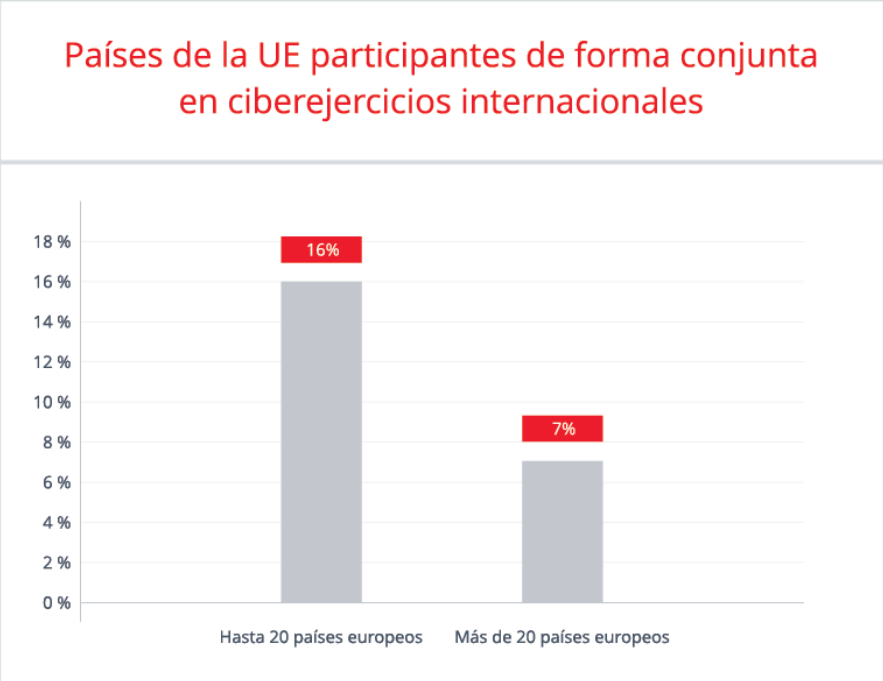

Figura 6. Países de la UE participantes de forma conjunta en ciberejercicios internacionales

Figura 7. Países participantes por año en ciberejercicios internacionales

- Número de ciberejercicios en los que ha participado España

La participación de España se refleja en un total de 21 ciberejercicios, de los cuáles, 11 pertenecen a ediciones de ciberejercicios internacionales y el resto, los celebrados dentro del ámbito nacional.

Se comprueba la cooperación y coordinación de España con el resto de países de su entorno, ya sean por la parte Europea o por la parte de la alianza Atlántica.

Figura 8. Número de ciberejercicios en los que ha participado España

Figura 9. Número de ciberejercicios por año con la participación de España

3.4.2 Sectores implicados

Se ha considerado de interés analizar la involucración en los ejercicios de participantes pertenecientes a sectores verticales, así como la implicación del sector público y/o privado.

Como sectores verticales, se han considerado los distintos sectores estratégicos definidos en la Ley 8/2011 por la que se establecen medidas para la protección de las infraestructuras críticas[7] [8] , es decir:

- Transporte.
- Energía.
- Financiero.
- Agua.
- Salud.

[7] http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630
[8] http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-8849

- TIC (Tecnologías de la Información y Comunicaciones).
- Químico.
- Nuclear.
- I+D.
- Alimentación.
- Espacio.
- Administración Pública.

- Sectores verticales implicados en los ciberejercicios

Se ha comprobado que, como era de esperar en ejercicios que tratan sobre las TIC, el sector más implicado en los ciberejercicios es el propio sector, cuyo compromiso se ha identificado en 27 ciberejercicios, seguido de los sectores de Finanzas, Transporte y Energía.

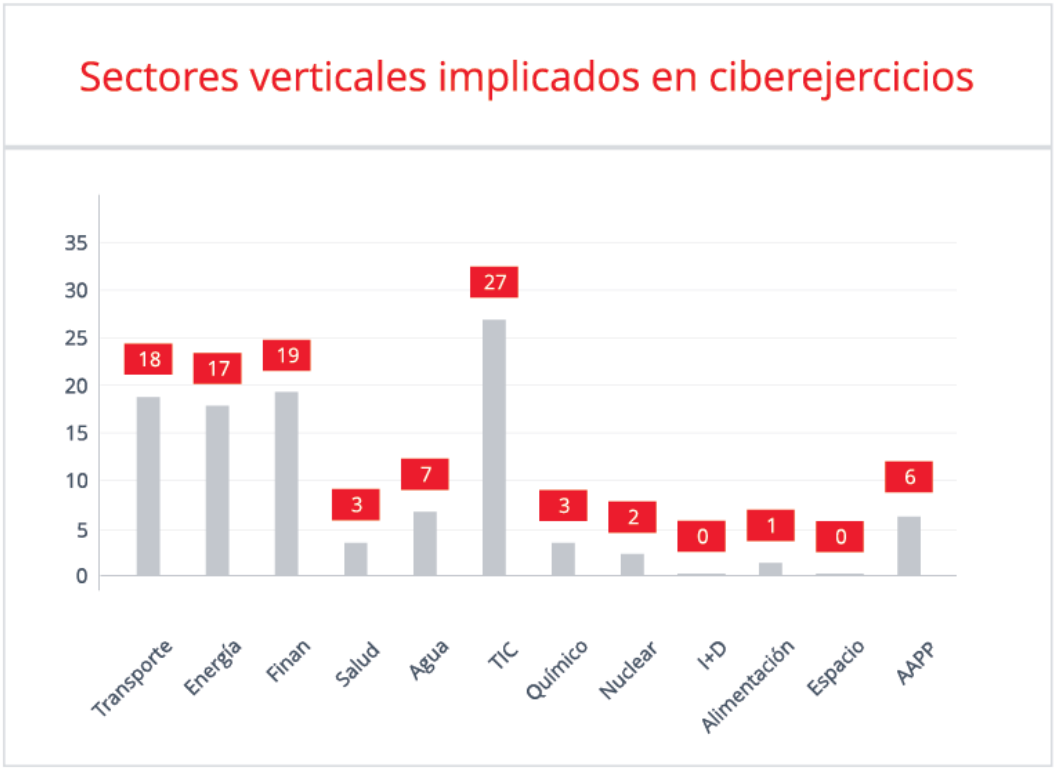

Figura 10. Sectores verticales implicados en los ciberejercicios

- Sectores verticales implicados de forma conjunta

Además de analizar el número de ciberejercicios en los que están implicados cada uno de los sectores descritos anteriormente, se considera interesante identificar aquellos que involucran a varios sectores conjuntamente. Para ello, se ha diferenciado entre aquellos ciberejercicios que involucran a un único sector, frente a aquellos que involucran a tres o más sectores verticales.

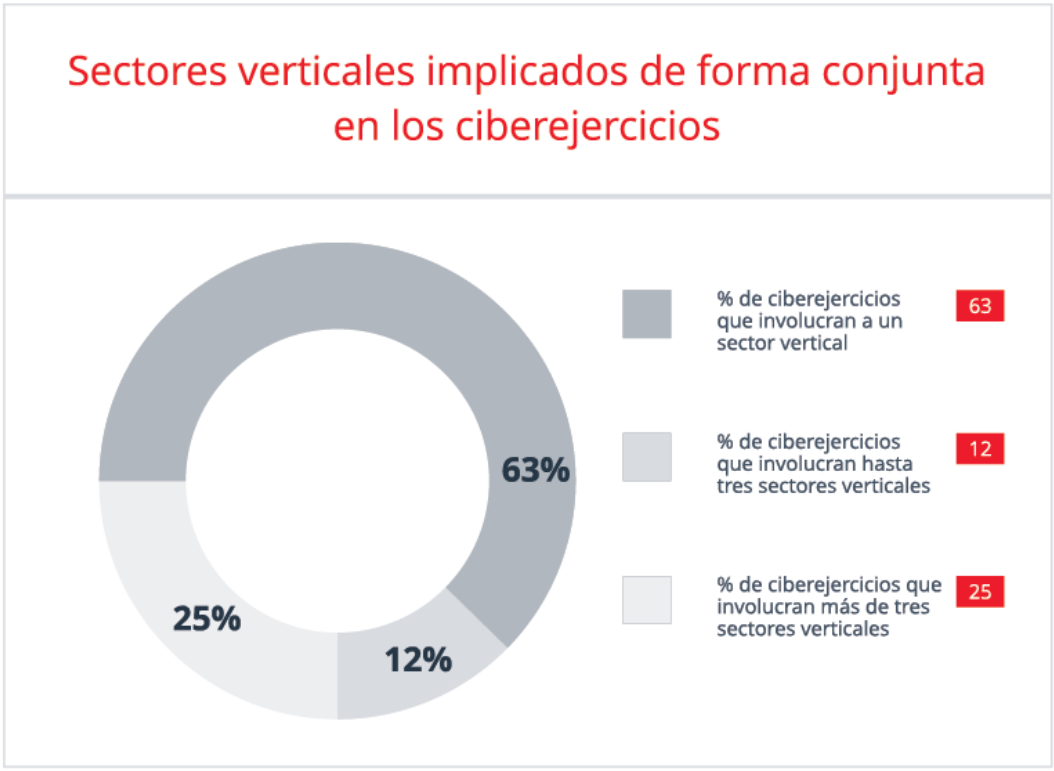

Figura 11. Sectores verticales implicados de forma conjunta en los ciberejercicios

- Sectores público y privado implicados en los ciberejercicios

Del mismo modo, se ha analizado la implicación de entidades públicas y privadas, teniendo en cuenta que los ciberejercicios pueden involucrar a ambos tipos, por lo que los resultados de la gráfica siguiente no tienen por qué resultar el 100%.

Se ha detectado que el 50% de los ciberejercicios involucra solo al sector público, frente al 5% que implica solo al sector privado; el 45% de los ciberejercicios compromete a ambos sectores.

Aunque inicialmente el sector público y el privado no participaban conjuntamente en ciberejercicios, actualmente se ha convertido en la práctica habitual, e incluso deseable.

Si participa solamente el sector público, suele responder a la necesidad de iniciar o mejorar las capacidades nacionales relacionadas con la seguridad en el ciberespacio antes de involucrar al sector privado. También puede responder a que el ámbito del ejercicio se ciñe al entorno militar.

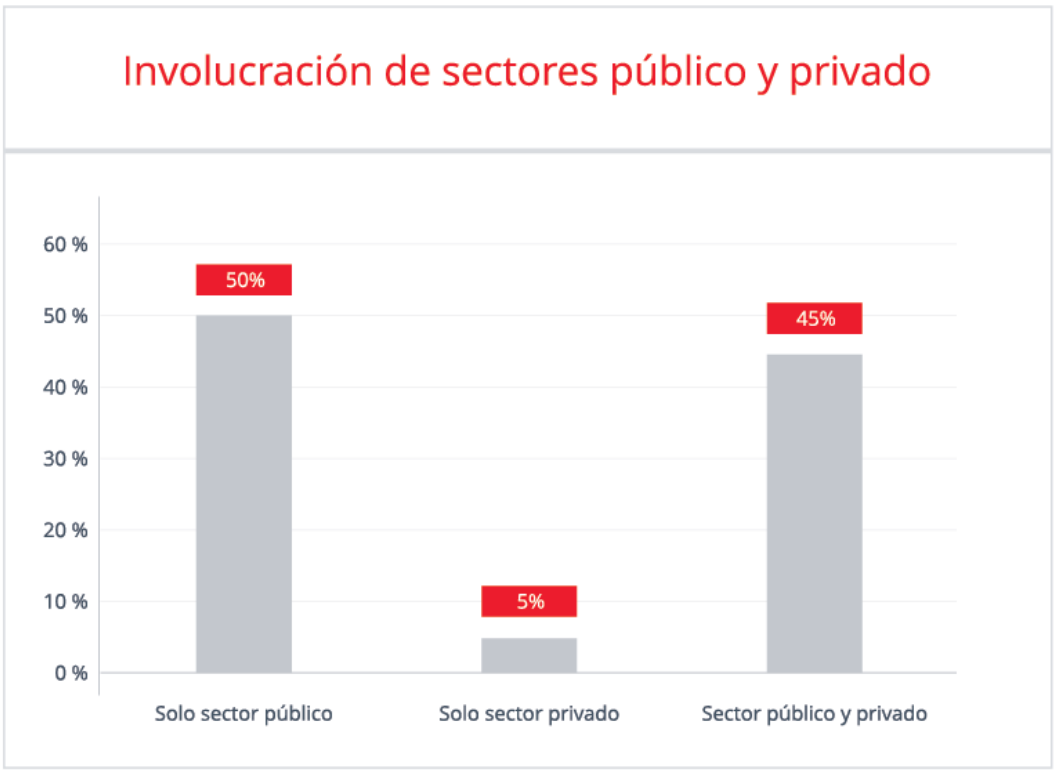

Figura 12. Sectores público y privado implicados en los ciberejercicios

3.4.3 Modalidad de Ciberejercicios

Atendiendo a cómo se llevan a cabo y en qué consisten los ciberejercicios, éstos pueden pertenecer a una modalidad diferente.

Unos son los llamados *tabletop*, que consisten en debates sobre hipotéticos escenarios en un ambiente informal, con el objetivo de evaluar los planes, las políticas y los procedimientos, o los sistemas necesarios para la prevención, respuesta y recuperación ante un determinado incidente.

Otra modalidad de ciberejercicios son los denominados de escala real. Estos son más complejos, ya que involucran a diversas organizaciones y jurisdicciones, con el objetivo

de validar muchos aspectos, como la implementación y el análisis de los planes, políticas, procedimientos y acuerdos de cooperación desarrollados en los ejercicios basados en debates.

La siguiente gráfica presenta información relativa a los ciberejercicios basados en *tabletop* y escala real, que son los únicos tipos que se han identificado en la información recopilada, por haber sido reportados explícitamente.

De la información recopilada sobre los ciberejercicios realizados, se puede concluir que un 35% de los ciberejercicios analizados declaran la realización de ejercicios con la modalidad *tabletop*, frente a un 6% de ciberejercicios que declaran la realización de ejercicios con la modalidad escala real. La facilidad de ejecución y el menor coste de los ciberejercicios *tabletop* puede ser el principal motivo de que sean los más utilizados. Como cada realización de un ciberejercicio puede ejecutar distintas modalidades de ejercicio, el cómputo global de los porcentajes sobre el total de los mismos no tiene que corresponderse con 100, pudiendo cada ciberejercicio aparecer en más de una modalidad.

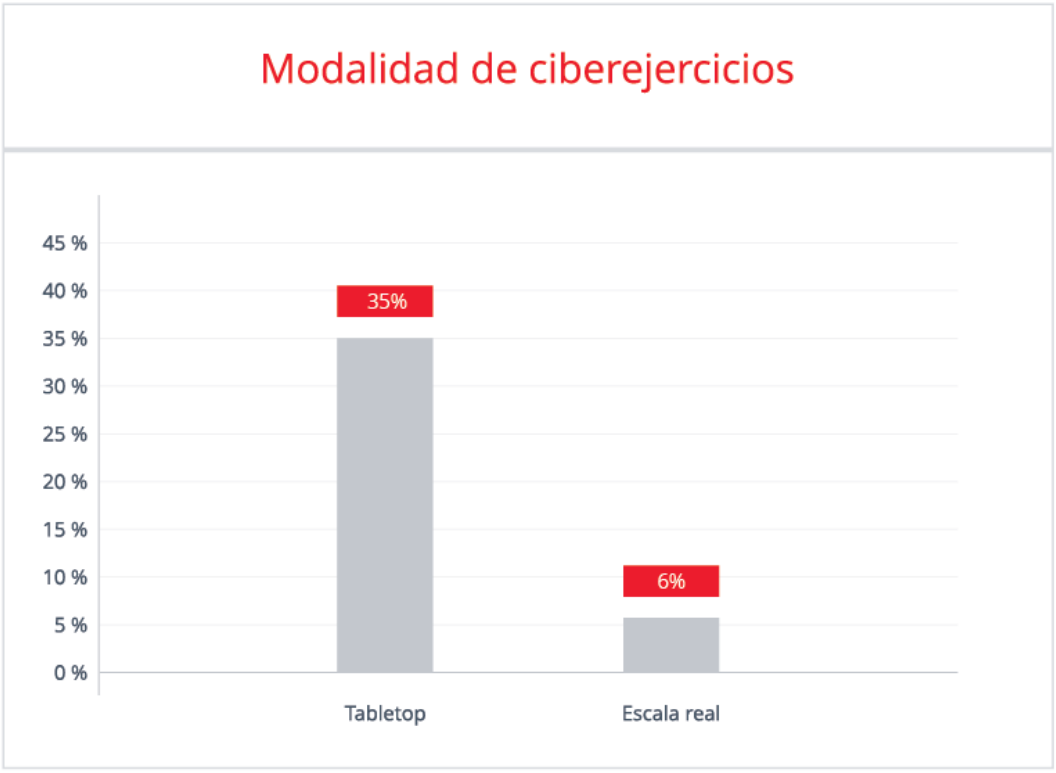

Figura 13. Modalidad de ciberejercicios

3.4.4 Evolución temporal de los ciberejercicios

- Número de ciberejercicios por año

En relación al número de ciberejercicios celebrados a lo largo del tiempo, vemos un claro aumento del número de ciberejercicios en los últimos años, llegando a los 26 celebrados en 2012, el año más prolífico. Sin embargo, también se observa un ligero descenso en los dos últimos años. Las causas de este descenso no han sido analizadas en profundidad en este documento, aunque debe considerarse que el presente estudio se ha realizado sin haber concluido el año 2014 y que se ha basado en gran parte en la información disponible sobre la implantación de la Agenda Digital y del informe de ENISA, ambos del año 2012.

Figura 14. Número de ciberejercicios por año

- Regularidad de los ciberejercicios

En cuanto a la regularidad de los ciberejercicios, se han analizado aquellos que se han celebrado sólo una vez, frente aquellos que han tenido varias ediciones a lo largo de los años, con una regularidad en el tiempo.

Se concluye que un 49% de los ciberejercicios se han celebrado más de una vez y de manera regular, lo que indica un compromiso de continuidad, con el consecuente proceso de mejora de cada nuevo ciberejercicio en el tiempo y también probablemente una de las causas de "conservar" el ciberejercicio es porque la amenaza u objeto sigue siendo válido.

Figura 15. Regularidad de los ciberejercicios

3.4.5 Ciberejercicios incluidos en la Agenda Digital para Europa

Conocer los ejercicios que están incluidos en la implementación de la Agenda Digital para Europa, proporciona información acerca de cuáles son significativos para cada uno de los países miembros. Del análisis realizado cabe destacar que más del 80% de los ciberejercicios analizados no están incluidos en la Agenda Digital para Europa.

Figura 16. Ciberejercicios incluidos en la Agenda Digital para Europa

3.4.6 Fases del incidente cubiertas por los ciberejercicios

El ciberejercicio puede estar centrado en una o varias de las fases de un posible incidente: la fase previa, durante o después del mismo.

Se ha considerado importante identificar qué fases han sido cubiertas en los ciberejercicios, concluyendo que todas las fases se han contemplado únicamente en el 20% de los casos, mientras que la mayoría de los ciberejercicios se centran únicamente en el momento de ocurrencia del incidente (55%). Debe tenerse en cuenta, que un ciberejercicio puede cubrir varias fases, pudiendo haber un ciberejercicio que quede representado en distintas fases de la gráfica, por lo que el total no es necesariamente el 100%.

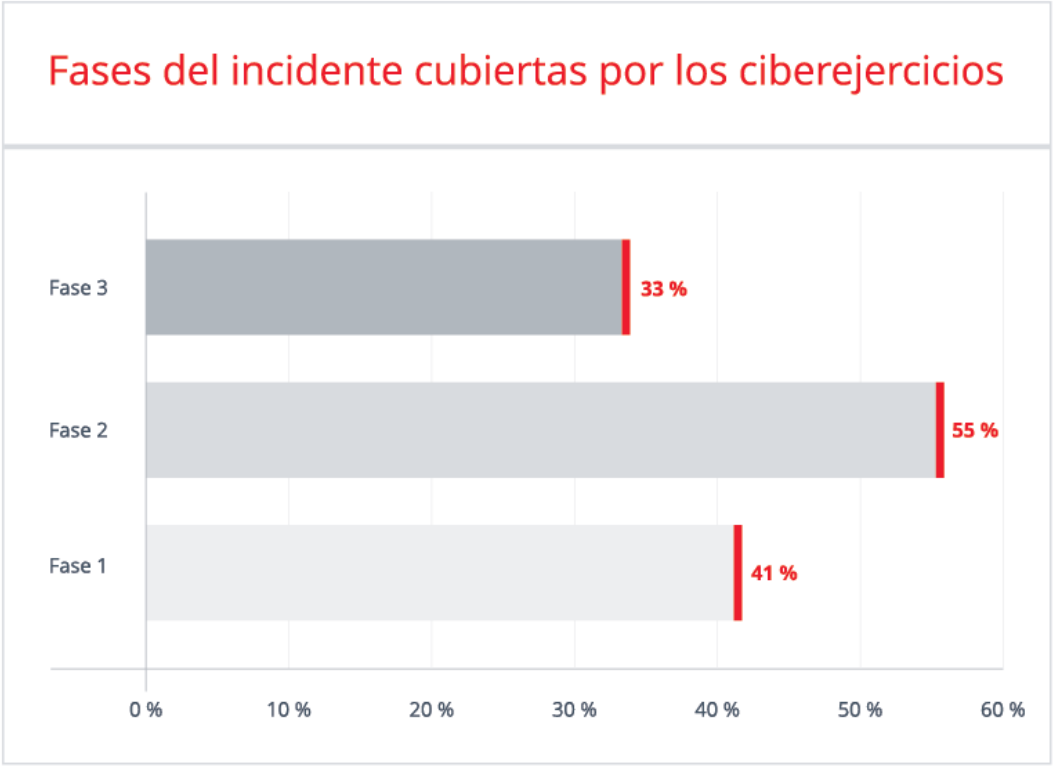

Figura 17. Fases del incidente cubiertas por los ciberejercicios

En este aspecto destaca la actuación de EEUU, que es la nación que con más frecuencia incluye todas las fases del incidente en los ciberejercicios que celebra.

3.4.7 Grado de participación de los países miembros

La siguiente gráfica presenta algunos ejemplos acerca del grado de participación de los países miembros de la UE en los ciberejercicios internacionales, que involucran a más de una nación.

Se ha establecido una diferenciación entre aquellos países que tienen una alta participación en los ciberejercicios internacionales (como por ejemplo Estonia, Alemania o Austria), frente aquellos que tienen una participación media (como por ejemplo Italia, España o Francia).

Cabe destacar, a modo de ejemplo, la participación de Alemania, tanto en ciberejercicios internacionales organizados por países europeos, como por otros países como EEUU *(Cyber Storm III*) o en la zona Asiática (*APCERT Drill 2014*).

Figura 18. Grado de participación de los países miembros en ciberejercicios internacionales

4 CIBEREJERCICIOS: PROPUESTA DE TAXONOMÍA

A partir del análisis y perfilado de los ciberejercicios, y tomando como referencia los trabajos realizados por dos organizaciones de distinta influencia geográfica como son ENISA y APEC[9] , se ha elaborado una taxonomía de los mismos, formada por cinco componentes principales, que se pueden observar en la figura siguiente:

9 http://www.mtc.gob.pe/portal/apectel38/spsg/08_tel38_spsg_013_APEC_Draft_Exercise_Report%5B1%5D.pdf

Figura 19. Componentes principales Taxonomía.

1. **Enfoque**

   El enfoque hace referencia al objetivo del ciberejercicio, identificando el propósito para el que ha sido realizado (por ejemplo concienciar, mejorar, etc.), así como qué aspectos intenta evaluar (planes, procedimientos, etc.) y qué fases del incidente cubre (antes de que ocurra, durante el incidente o después de su ocurrencia).

2. **Modelo**

   En este componente se recogen los distintos modelos de ejecución en los que se basan los ejercicios, ya sean basados en debates entre los participantes (por ejemplo tabletop, juegos, talleres, etc.), o en las operaciones de los participantes (por ejemplo escala real, simulacros, etc.).

3. **Sector Vertical**

   Su finalidad es plasmar los distintos sectores en los que aplicaría al ciberejercicio, teniendo en cuenta los sectores estratégicos definidos por la reglamentación PIC (Protección de Infraestructuras Críticas)[10] [11]en España.

4. **Ámbito Participación**

   En este componente se recoge la procedencia de los participantes, tanto a nivel geográfico, como a nivel de sectores públicos y/o privados, y de rol que desempeñan los participantes (por ejemplo técnicos, gestores o directivos).

5. **Difusión Resultados**

   Se recoge el nivel de difusión que se aplica a los resultados, en el sentido de si son accesibles al público, o se difunden de manera privada.

[10] http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630
[11] http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-8849

En la siguiente figura se reflejan todos los campos de la taxonomía propuesta y en las siguientes secciones se describe cada componente principal.

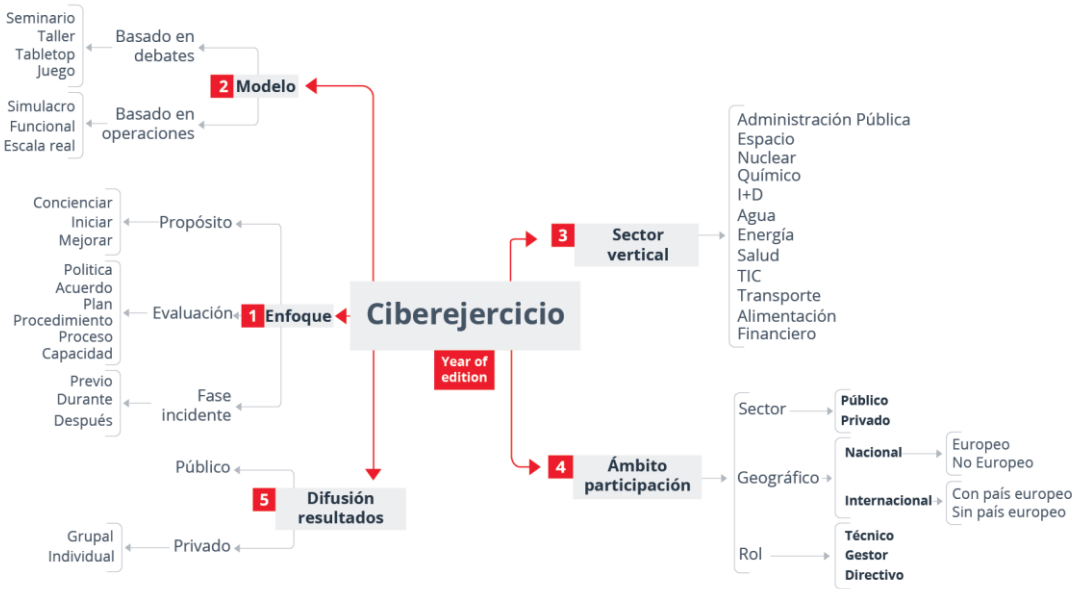

Figura 20. Esquema Taxonomía Ciberejercicios.

4.1 ENFOQUE

Dentro del enfoque del ciberejercicio, se han considerado tres grandes apartados: la fase del incidente que se tratará, qué es lo que se evaluará y con qué propósito.

Figura 21. Componente Enfoque.

- **Propósito**

El propósito del ciberejercicio, puede ser para concienciar, iniciar / establecer algunas tareas o acciones dentro de una organización o mejorar algunas tareas o acciones existentes dentro de una organización.

- **Evaluación**

Habitualmente los ejercicios se suelen realizar para evaluar ciertas tareas o acciones dentro de una organización que tienen su aplicación en alguna de las fases de un incidente, como una política (que afecte a un país, a una organización, sobre intercambio de información, de la seguridad, etc.), un acuerdo (de colaboración, de cooperación, de ayuda mutua, etc.), un plan (por ejemplo, planes de respuesta), un procedimiento (como por ejemplo los SOPs), un proceso (por ejemplo para evaluar la eficiencia dentro de una organización) o una capacidad determinada (por ejemplo, los conocimientos de los participantes).

- **Fase Incidente**

El ciberejercicio puede estar centrado en la fase previa al incidente, durante el incidente o después del incidente, pudiendo cubrir varias fases.

4.2 MODELO

De los modelos propuestos por ENISA, el de tipo *tabletop* y el de escala real (*full simulation*) cubrían un grupo importante de los ciberejercicios que habían identificado (un 62%), mientras que un 22% de los ciberejercicios se correspondía con el modelo "otro" ciberejercicio. Sin embargo, al revisar la especificación de los modelos de la APEC, se ha comprobado que pueden encajar tanto los modelos definidos por ENISA (los que tienen el mismo nombre es trivial el encaje, y el resto de los modelos encajan como realizaciones específicas de simulacros), como las distintas realizaciones de los ciberejercicios que se han recopilado.

Figura 22. Componente Modelo.

- **Basado en Debates**

Se utilizan como los primeros ejercicios a realizar dentro de una organización para, progresivamente, ir aumentando la complejidad. Este modelo de ejercicios suelen centrarse en cuestiones estratégicas permitiendo familiarizarse con capacidades actuales o previstas de una entidad ya sea planes, políticas, acuerdos o procedimientos. Dentro de este modelo de ejercicios se encuentra el seminario, el taller, el tabletop y el juego.

a. Seminario

Los seminarios son debates informales que proporcionan una visión general a los participantes. Los seminarios son un punto de partida para desarrollar o hacer importantes cambios a los planes y procedimientos de una organización.

b. Taller

Los talleres se centran en la consecución o el desarrollo de un resultado en concreto, cuánto más específico, más eficaz será.

c. **Tabletop**

Se debate con las personas clave sobre hipotéticos escenarios en un ambiente informal, con el objetivo de evaluar los planes, las políticas y los procedimientos, o para evaluar los sistemas necesarios para abordar las fases de un incidente.

d. **Juego**

En un juego se describe una situación real o supuesta. El objetivo del juego consiste en explorar el proceso de la toma de decisiones y sus consecuencias, sin usar recursos reales.

- **Basado en Operaciones**

Se utilizan para validar los planes, políticas, acuerdos y procedimientos consolidados en los ejercicios basados en debates. Este modelo de ejercicios permite aclarar las funciones y las responsabilidades, identificar las lagunas para implementar los planes y procedimientos, y mejorar el rendimiento individual y colectivo. Dentro de este modelo de ejercicios se encuentra el simulacro, el ejercicio funcional y el ejercicio a escala real.

a. **Simulacro**

Los simulacros se suelen emplear para validar una operación o una función específica en una determinada organización. Los simulacros se suelen utilizar para formar nuevos equipos, para desarrollar o validar nuevas políticas o procedimientos, o para practicar y mantener las habilidades actuales.

b. **Funcional**

Los ejercicios funcionales están diseñados para validar y evaluar las capacidades individuales, y para probar los planes, las políticas, los procedimientos y el personal de una organización. Este tipo de ejercicio estimula las operaciones en un área funcional, presentando problemas complejos y reales que requieren respuestas rápidas y eficaces en un entorno estresante y con limitaciones de tiempo.

c. **Escala real**

Este tipo de ejercicio es el más complejo. Se suelen centrar en la implementación y el análisis de los planes, políticas, procedimientos y acuerdos de cooperación desarrollados en los ejercicios basados en debates y perfeccionados en ejercicios anteriores basados en operaciones más pequeños. El nivel de apoyo y la financiación necesaria para llevar a cabo este tipo de ejercicio es mayor que cualquier otro tipo de ejercicio.

4.3 SECTOR VERTICAL

Se ha considerado como sector vertical los distintos sectores estratégicos definidos en la Ley 8/2011 [12] por la que se establecen medidas para la protección de las infraestructuras críticas. El sector TIC ha sido el que más ha aparecido implicado en los ciberejercicios.

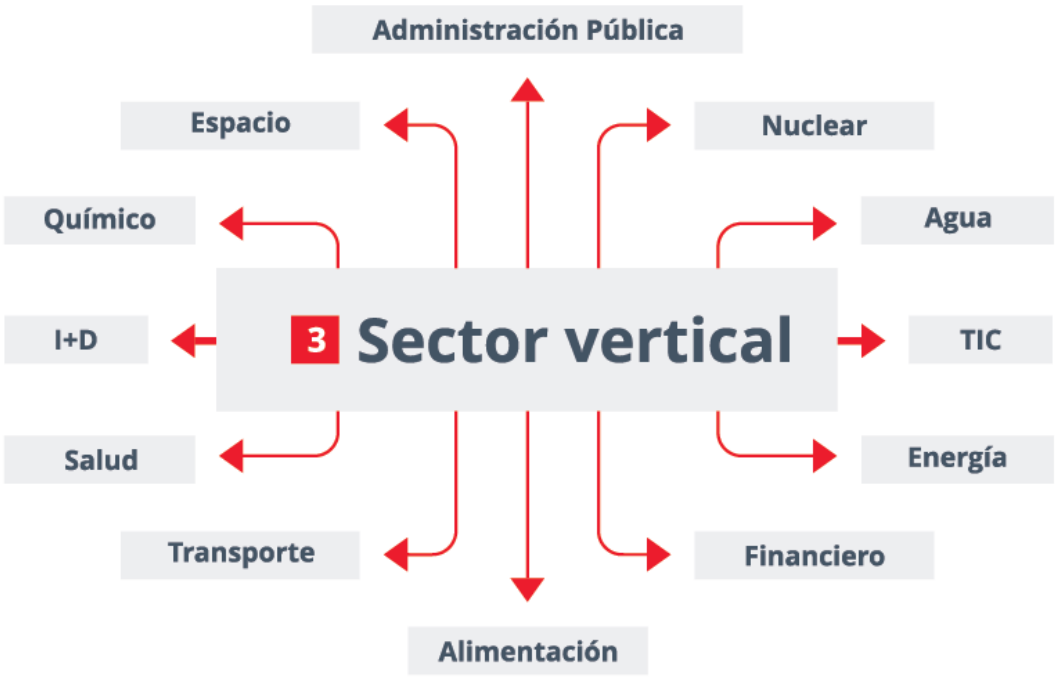

Figura 23. Componente Sector Vertical.

4.4 ÁMBITO PARTICIPACIÓN

Este módulo está orientado a perfilar la participación de las personas durante el ciberejercicio, para ello se tiene en cuenta su pertenencia sectorial (público o privado), su ubicación geográfica y el rol desempeñado dentro de su organización.

[12] http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630

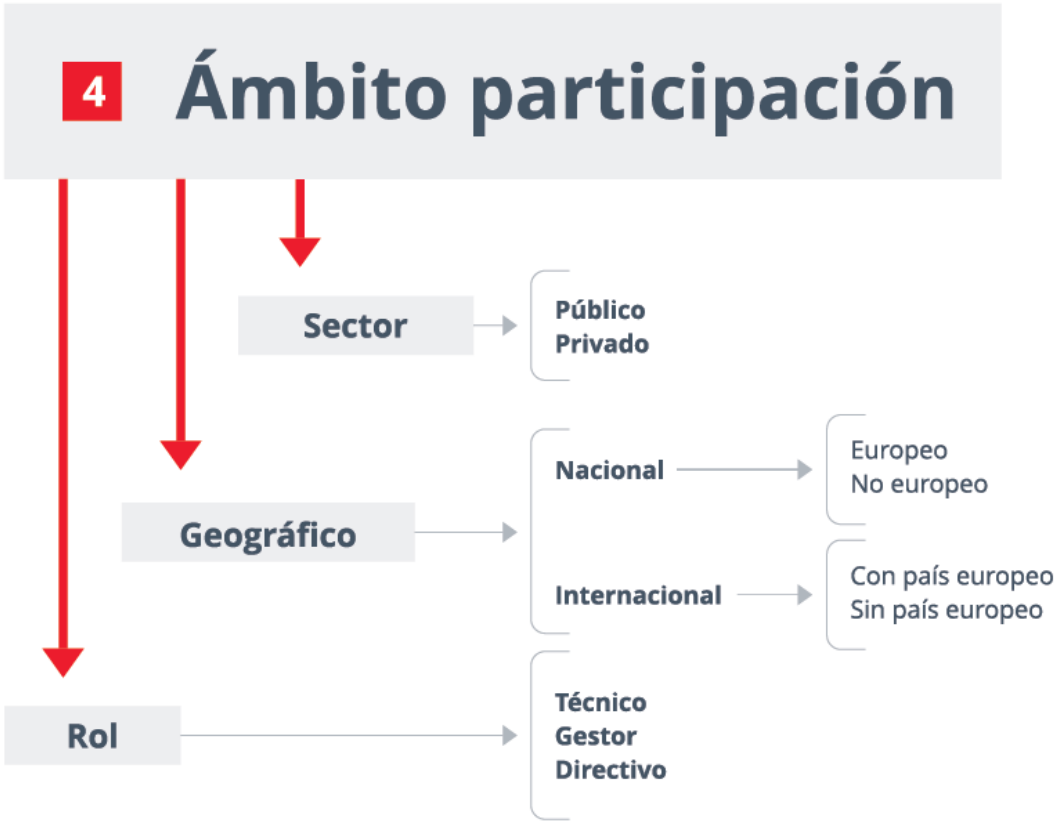

Figura 24. Componente Ámbito Participación.

- **Sector**

  El participante puede pertenecer del sector privado o público dentro de los distintos sectores verticales a los que está enfocado el ciberejercicio.

- **Geográfico**

  El ámbito geográfico del ejercicio puede ser nacional o internacional, haciendo especial hincapié en la existencia de algún país europeo en el mismo.

- **Rol**

  Dependiendo del enfoque del ciberejercicio, se requiere la participación de diversos perfiles de cada organización, distinguiéndose entre técnicos, gestores o directivos.

4.5 DIFUSIÓN RESULTADOS

Dentro de la difusión de resultados, se ha podido constatar que existe una segregación de la información que se difunde tanto al público en general, como a ciertos grupos de participantes o a cada participante individualmente.

Figura 25. Componentes Difusión Resultados.

5 TAXONOMÍA APLICADA A LOS CIBEREJERCICIOS

Una vez construida la taxonomía, se ha seleccionado una serie de ciberejercicios relevantes de entre los recopilados, para obtener, de este modo, un ejemplo de la caracterización de los mismos.

5.1 SELECCIÓN DE CIBEREJERCICIOS

La selección de ciberejercicios responde principalmente a los resultados obtenidos de las métricas definidas previamente.

Se ha seleccionado una muestra relevante de los ciberejercicios celebrados recientemente. Los criterios de selección utilizados incluyen únicamente los últimos ciberejercicios que:

- Son de ámbito nacional en España.
- Incluyen la participación internacional de España, y están contenidos en la implementación de la Agenda Digital para Europa.

A los restantes ciberejercicios, que no se han seleccionado considerando los criterios previos, se les han aplicado los siguientes:

- Aquellos que se celebran de forma regular a lo largo del tiempo, y presentan la modalidad de escala real.
- Afectan a un único sector muy específico (finanzas o salud), y presentan, preferiblemente, la participación de países europeos.

La lista de las últimas ediciones de los ciberejercicios que han resultado relevantes después de aplicar los criterios de selección son:

EJERCICIO	AÑO
CYBER STORM	2013
LOCKED SHIELDS	2014
CYBER COALITION	2014
CYBERATLANTIC	2011
CYBEREUROPE	2014
EUROCYBEX	2011
EUROSOPEX	2012
CYBER-EX	2013
PSCIC	2014
EJERCICIO DE CIBERDEFENSA	2014
CYBERRX	2014
WAKING SHARK	2013

Tabla 5. Lista de ciberejercicios considerados relevantes

5.2 APLICACIÓN DE LA TAXONOMÍA

Las siguientes figuras reflejan la aplicación de la taxonomía a la selección realizada:

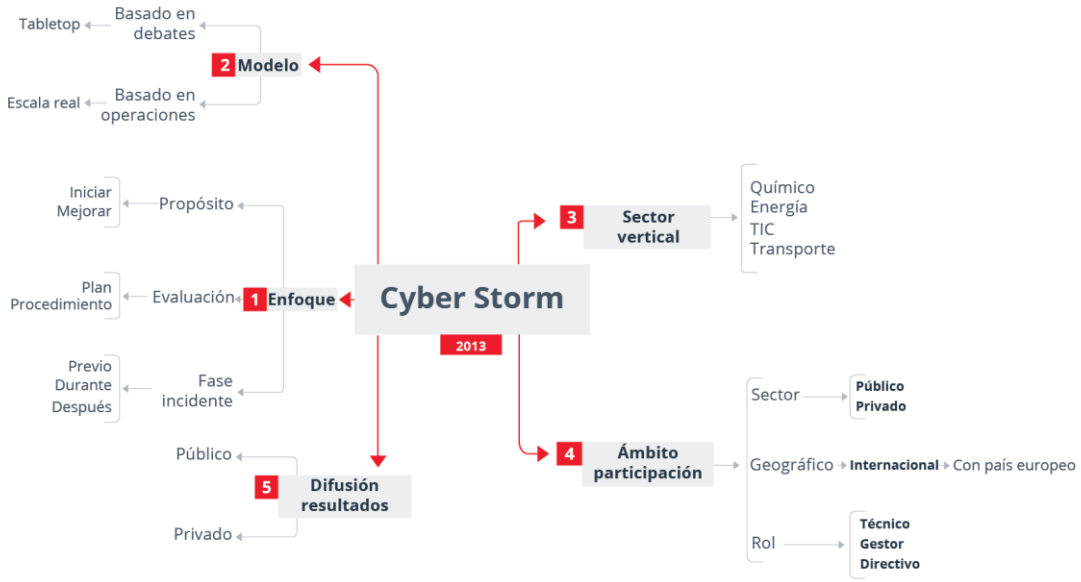

Figura 26. Esquema Taxonómico Cyber Storm 2013.

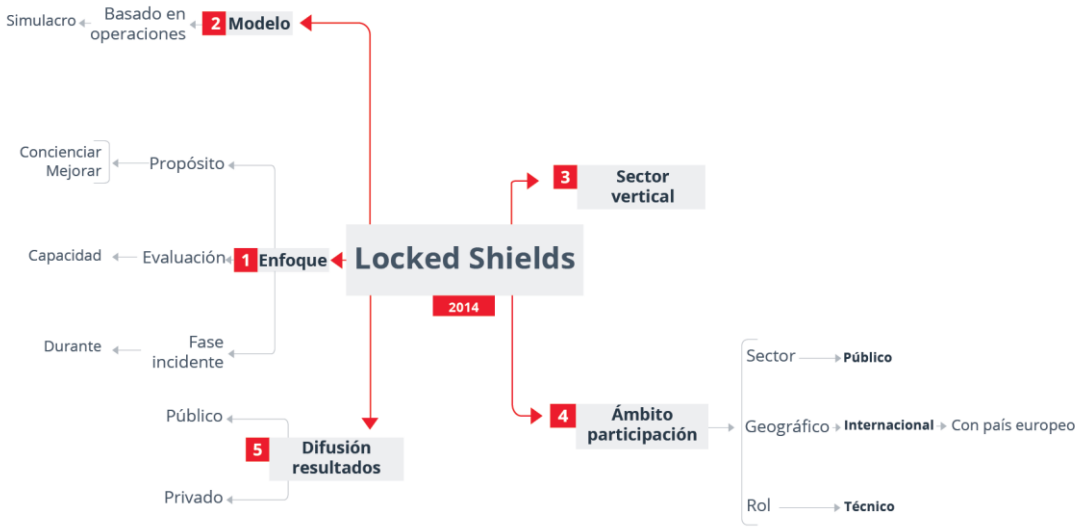

Figura 27. Esquema Taxonómico Locked Shields 2014.

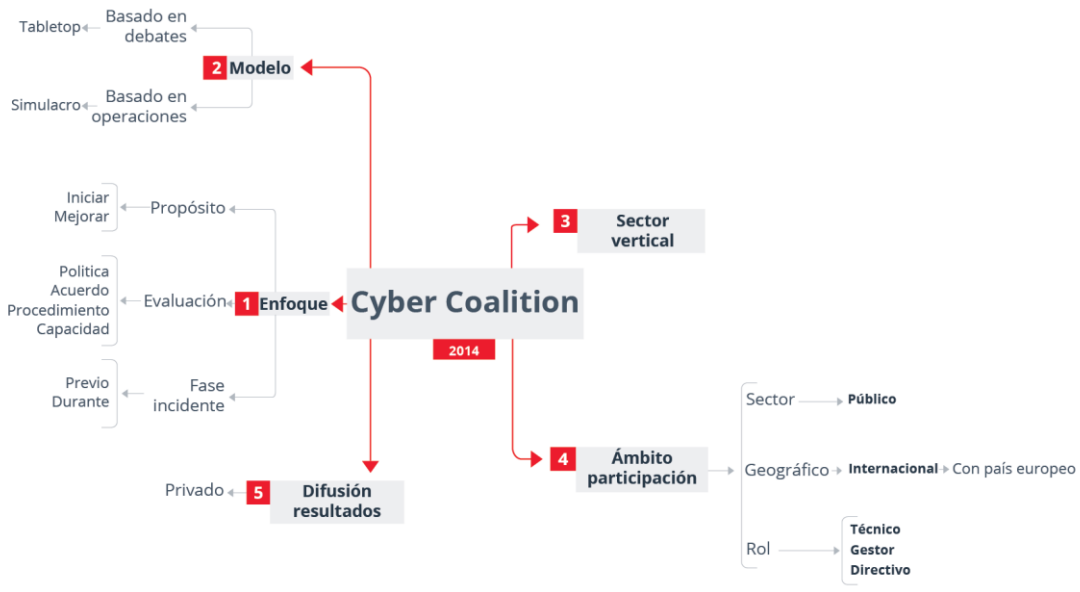

Figura 28. Esquema Taxonómico Cyber Coalition 2014.

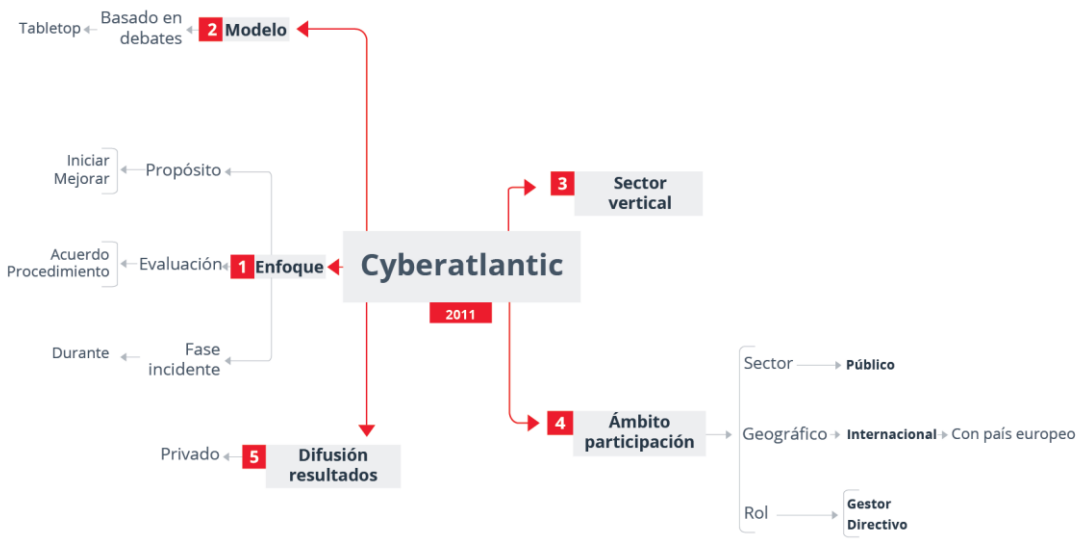

Figura 29. Esquema Taxonómico CyberAtlantic 2011.

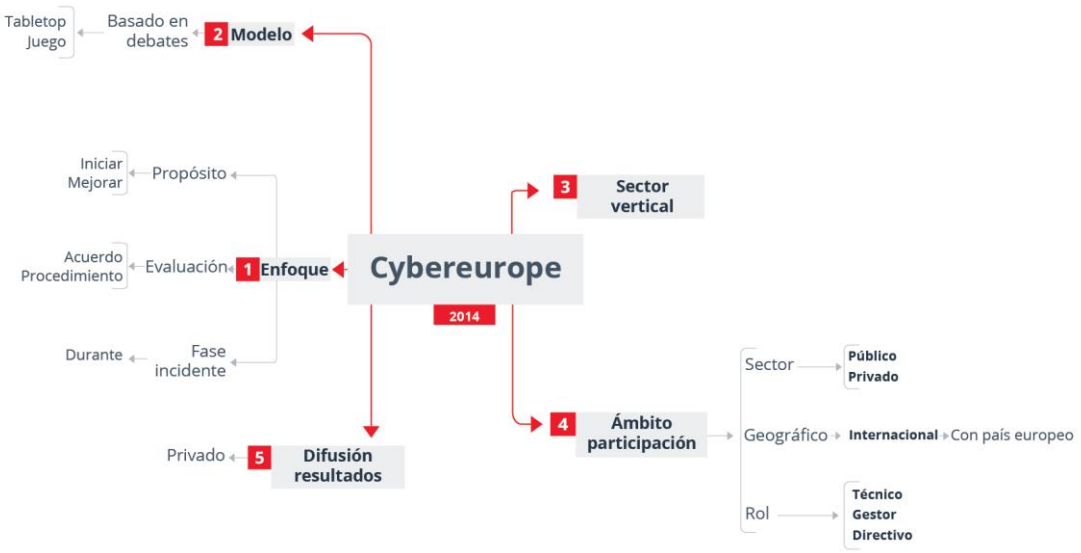

Figura 30. Esquema Taxonómico CyberEurope 2014.

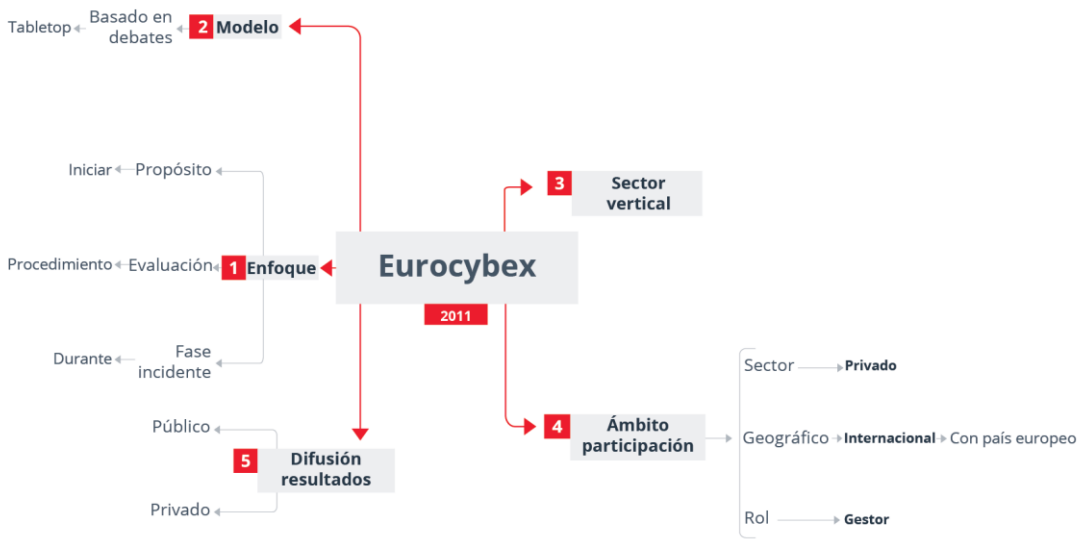

Figura 31. Esquema Taxonómico Eurocybex 2011.

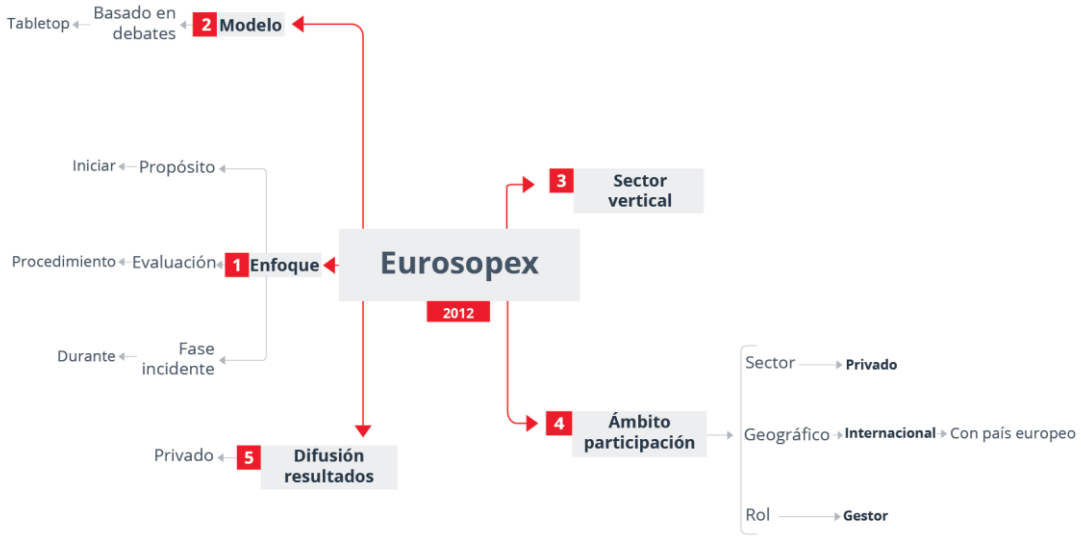

Figura 32. Esquema Taxonómico EuroSopex 2012.

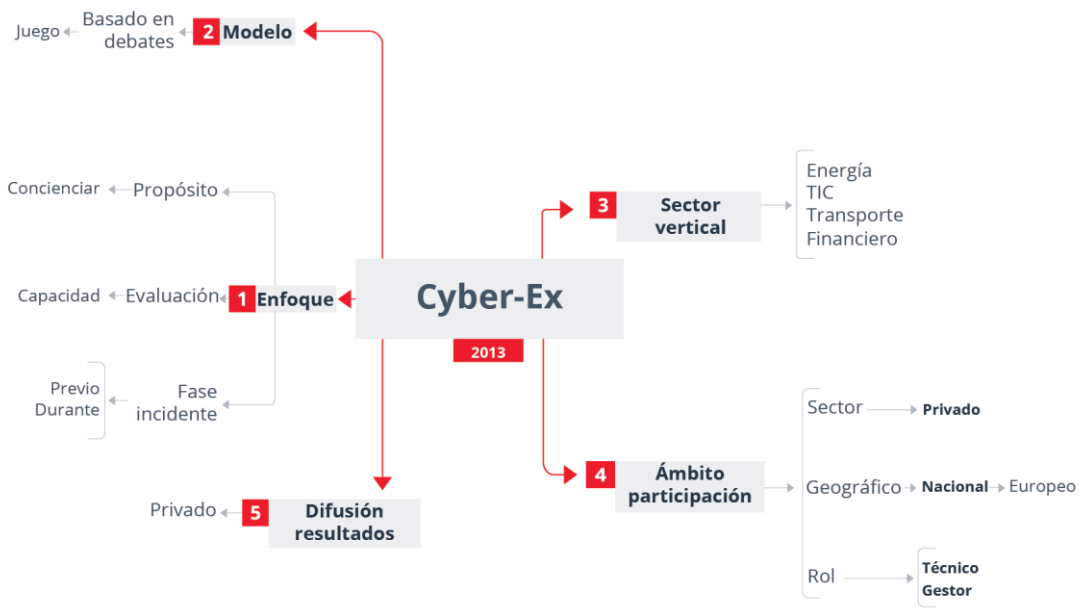

Figura 33. Esquema Taxonómico Cyber-Ex 2013.

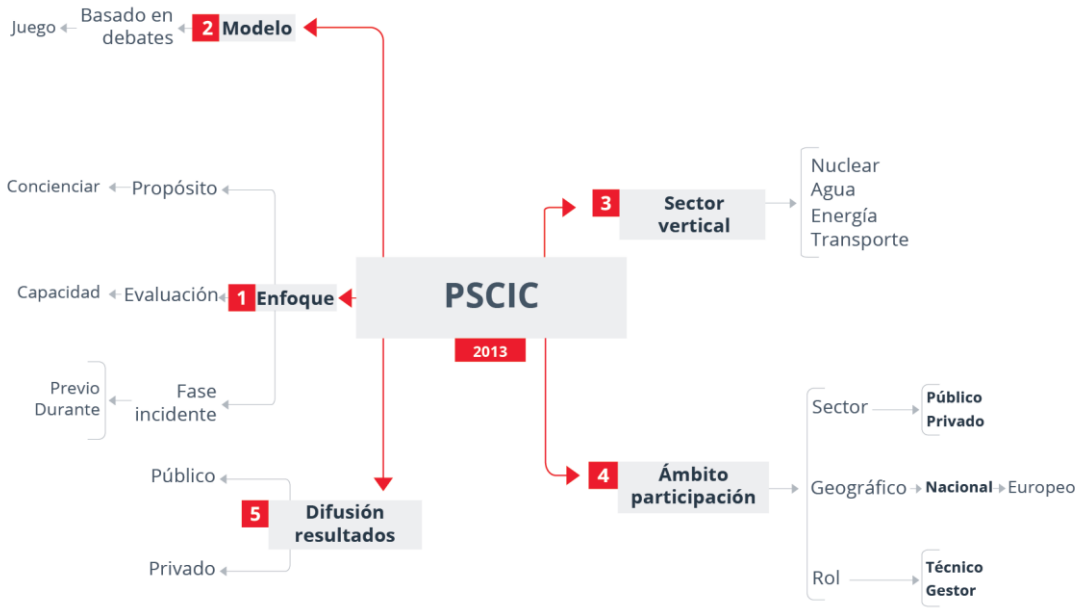

Figura 34. Esquema Taxonómico PSCIC 2014.

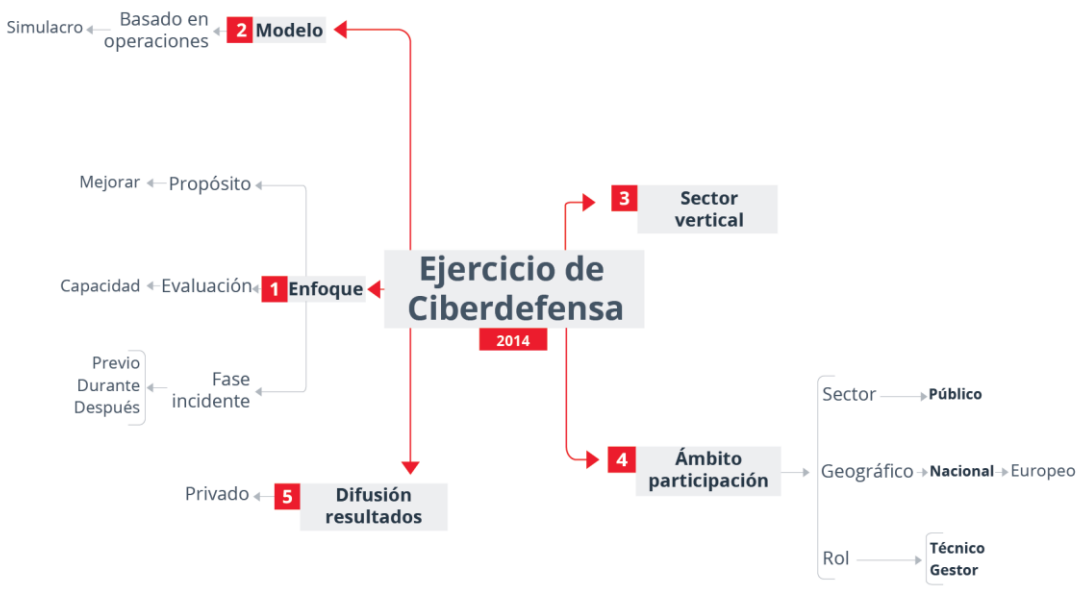

Figura 35. Esquema Taxonómico ECD 2014.

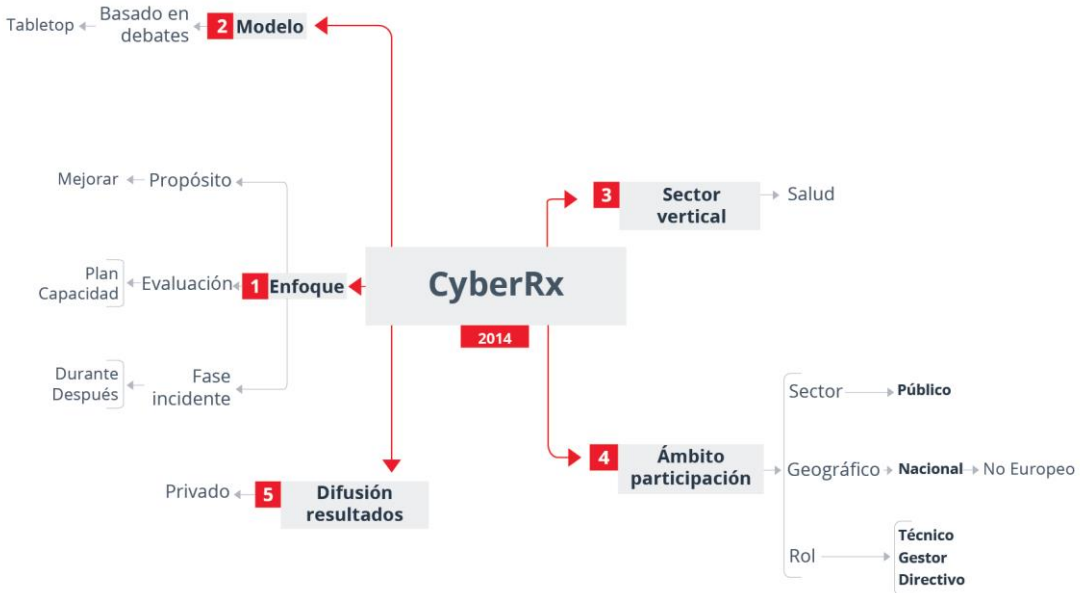

Figura 36. Esquema Taxonómico CyberRx 2014.

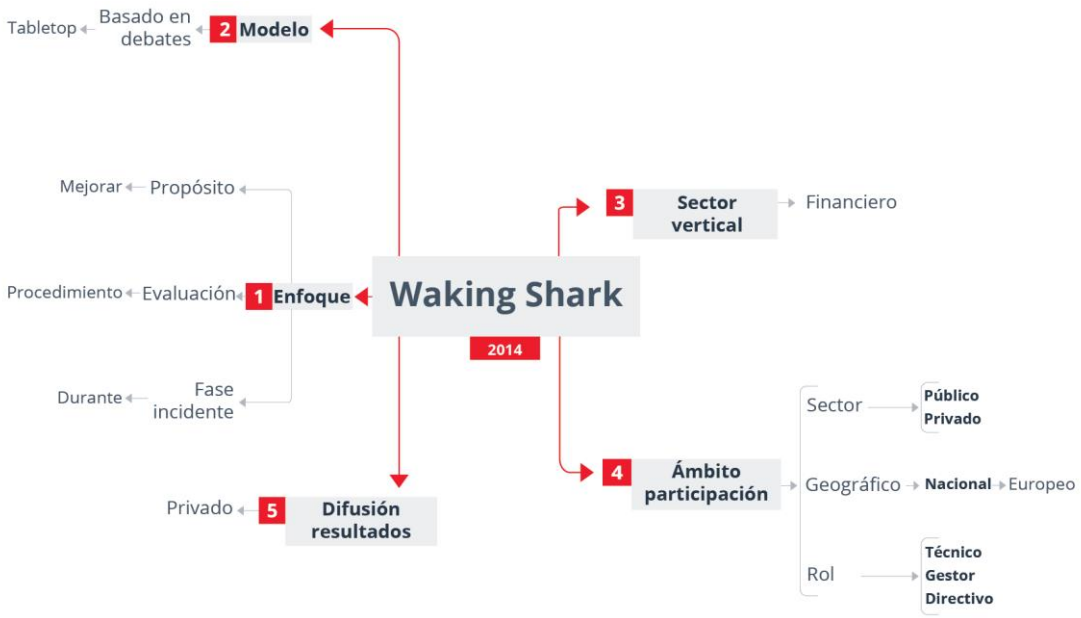

Figura 37. Esquema Taxonómico Waking Shark 2013.

La aplicación de la taxonomía a los ciberejercicios previos, permite establecer un mapa de ejecución de los mismos atendiendo a distintas caracterizaciones que se analizan en las siguientes subsecciones.

5.2.1 Perspectiva sectorial

Aunque las TIC están presentes y afectan a todos los sectores estratégicos, en el análisis sólo se han considerado ciberejercicios específicos del sector vertical TIC cuándo se afrontaba directamente como un servicio esencial proporcionado por los operadores TIC o se contaba con su participación. Se ha tomado esta decisión para tratar de mantener la coherencia con los sectores estratégicos identificados por la Ley PIC (8/2011).

Por ello, desde una perspectiva sectorial no se ha realizado una caracterización específica para un ciberejercicio cuándo éste no afronta específicamente un determinado sector vertical.

La siguiente figura vuelve a mostrar el número de veces que los sectores verticales han sido tratados en las distintas realizaciones de los ciberejercicios.

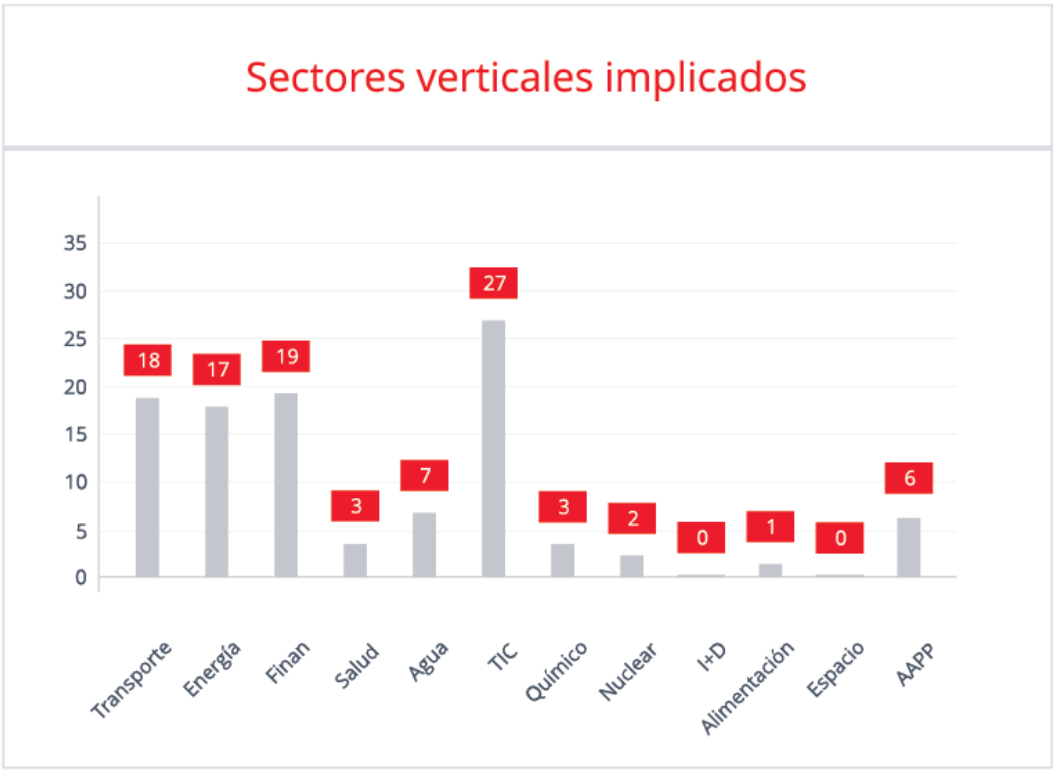

Figura 38. Sectores verticales implicados en los ciberejercicios.

Como se puede observar existen muchos ciberejercicios que abordan los sectores verticales de Transporte y Energía. Ambos sectores están identificados en la Directiva Europea sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección[13].

El sector TIC también se trata específicamente en los ciberejercicios con gran frecuencia, sector que se identificado en la Directiva Europea como el siguiente sector de aplicación en próximas revisiones de la Directiva.

La crisis financiera ha hecho mella en el auge de ciberejercicios en el sector financiero, haciendo crecer el número de ciberejercicios realizados que comprometen a dicho sector.

Sin embargo, no se ha constatado ningún ciberejercicio que tenga en cuenta el sector de I+D a pesar de la importancia que tiene este sector en época de crisis para dar valor añadido a la economía de cada país.

Tampoco se ha constatado ningún ciberejercicio focalizado en el sector del Espacio, a pesar de la dependencia existente en múltiples sectores con los servicios que suministra.

[13] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008L0114&from=ES

Sin embargo, en un documento de trabajo de la Comisión Europea dónde se aborda un nuevo acercamiento al programa de protección de infraestructuras críticas europeas[14], se seleccionan 4 infraestructuras específicas de dimensión europea, siendo una de ellas Galileo, el Programa europeo para un sistema global de navegación por satélite. Por ello se supone que en un futuro cercano se realizarán ciberejercicios que incluya al sector Espacio, y más concretamente el sistema Galileo.

El resto de sectores tiene una mínima representación en la realización de los ciberejercicios contemplados, lo cual parece indicar una cierta preocupación por los sectores correspondientes pero que tal vez necesita del impulso adecuado, ya sea por parte de las autoridades reguladoras o a una actualidad que demande con cierta premura la protección de ciertos servicios. Por ejemplo, y en línea con esto último, puede ser que los casos recientes de pandemias generen una demanda social en la protección de los servicios sanitarios que se soportan en sistemas TIC.

5.2.2 Modelos utilizados

Los modelos utilizados en los ciberejercicios son muy diversos, atendiendo a si están basados en debates, en operaciones o incluso una mezcla de ambos. El mayor número de ciberejercicios basados en debates, no es de extrañar, ya que son por los que habitualmente se empieza antes de desarrollar una capacidad operativa y que normalmente, requieren menos tiempo para su preparación.

La siguiente figura muestra el porcentaje de aparición de modelos de ejercicios en las distintas realizaciones, si bien debe resaltarse que algún ciberejercicio puede contener varios ejercicios del mismo modelo, por eso la suma de los porcentajes no corresponde al 100%.

14 http://ec.europa.eu/energy/infrastructure/doc/critical/20130828_epcip_commission_staff_working_document.pdf

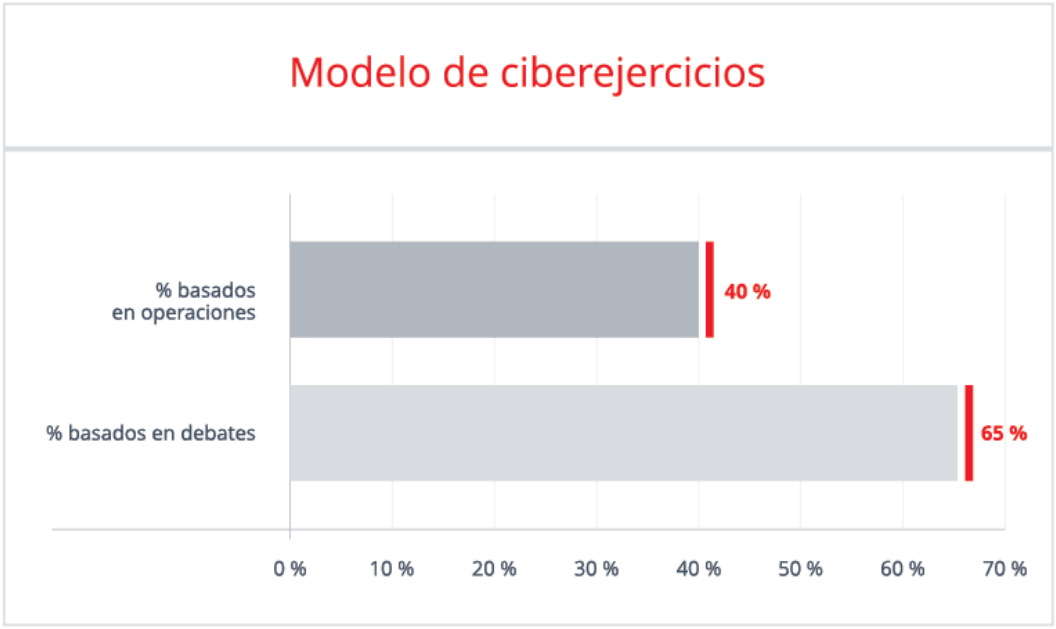

Figura 39. Porcentaje de aparición según el modelo de los ejercicios.

Si nos atenemos a los distintos escenarios en función de los modelos de ciberejercicios, se han detectado los que aparecen reflejados en la siguiente tabla:

MODELO DE CIBEREJERCICIOS	ESCENARIOS
DEBATES	TABLETOP
	TABLETOP + SEMINARIO
	TABLETOP + SEMINARIO + TALLER
	JUEGO
	TABLETOP + JUEGO
OPERACIONES	SIMULACRO
	ESCALA REAL
	FUNCIONAL
	FUNCIONAL + ESCALA REAL
MIXTOS	TABLETOP + ESCALA REAL

Tabla 6. Escenarios utilizados por modelo de los ejercicios

La siguiente figura representa el porcentaje de aparición de cada una de las modalidades dentro de modelo de ciberejercicios. Como en la anterior figura, se representa la aparición de cada modalidad en los ciberejercicios realizados, por lo que el cómputo global de los porcentajes no tiene que corresponderse con 100.

La mayor parte de los ciberejercicios realizados son de tipo *tabletop*, juegos o simulacros. Si bien es posible que muchos seminarios o talleres realizados no han sido contabilizados como ciberejercicios.

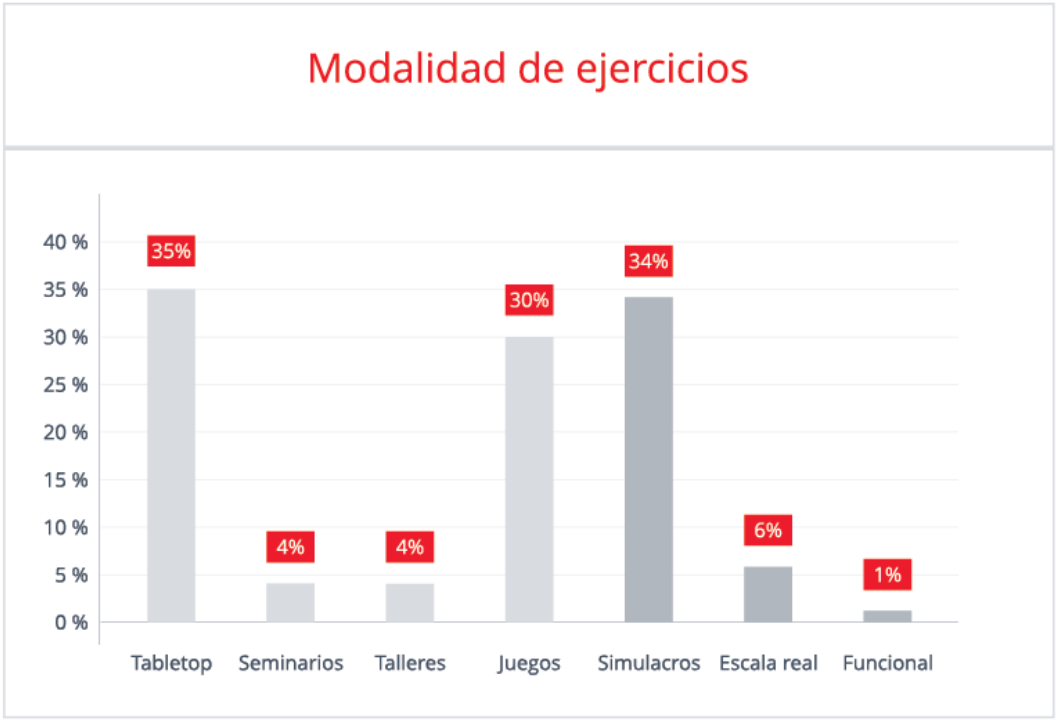

Figura 40. Porcentaje de aparición según la modalidad de los ejercicios.

Los ejercicios, independientemente de su modalidad, se suelen realizar para evaluar ciertas tareas o acciones dentro de una organización que tienen su aplicación en alguna de las fases de un incidente, como una política, un acuerdo, un plan, un procedimiento, un proceso o una capacidad determinada. La siguiente figura representa los porcentajes de aparición de los distintos aspectos evaluados en los ciberejercicios realizados sobre el total de los mismos, pudiendo cada ciberejercicio aparecer en más de una modalidad y por lo tanto el cómputo global de los porcentajes no tiene que corresponderse con

100. Es destacable el alto grado de aparición que tiene la capacidad, debido a que muchos ejercicios buscan el entrenamiento del personal.

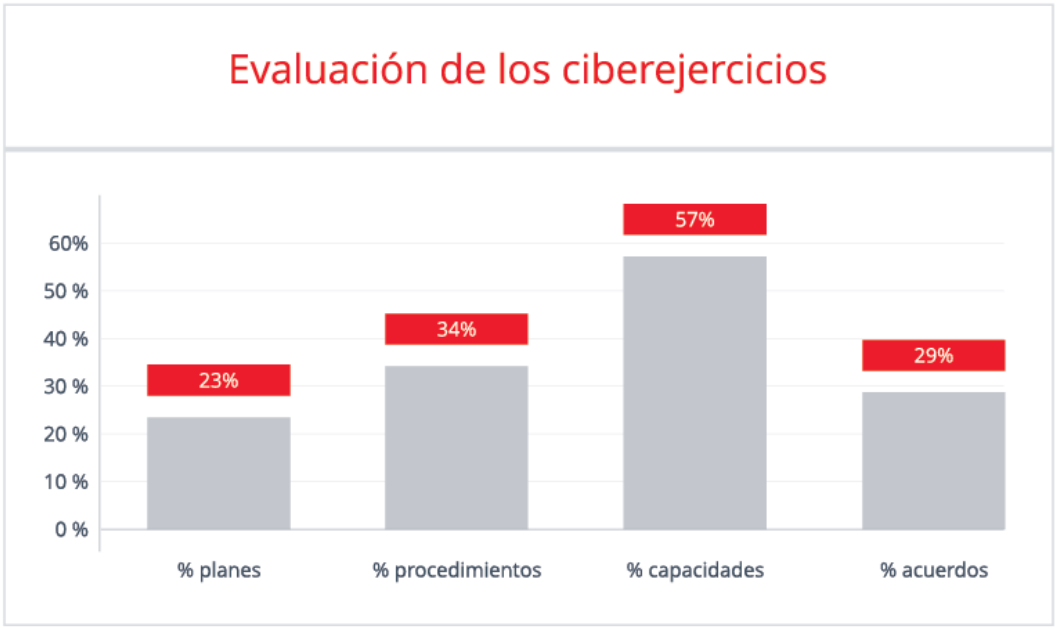

Figura 41. Porcentaje de aparición por evaluación de los ejercicios.

El propósito del ciberejercicio, puede ser concienciar, iniciar/establecer algunas tareas o acciones dentro de una organización, o mejorar algunas tareas o acciones dentro de una organización. La siguiente figura representa los porcentajes de aparición de los distintos propósitos perseguidos en los ciberejercicios realizados sobre el total de los mismos, pudiendo tener cada ejercicio varios propósitos, por lo que el cómputo global de los porcentajes de ocurrencia no tiene que corresponder con 100. Cabe destacar el propósito de mejora como el de mayor aparición, debido a que muchos ejercicios buscan la mejora del objeto de evaluación.

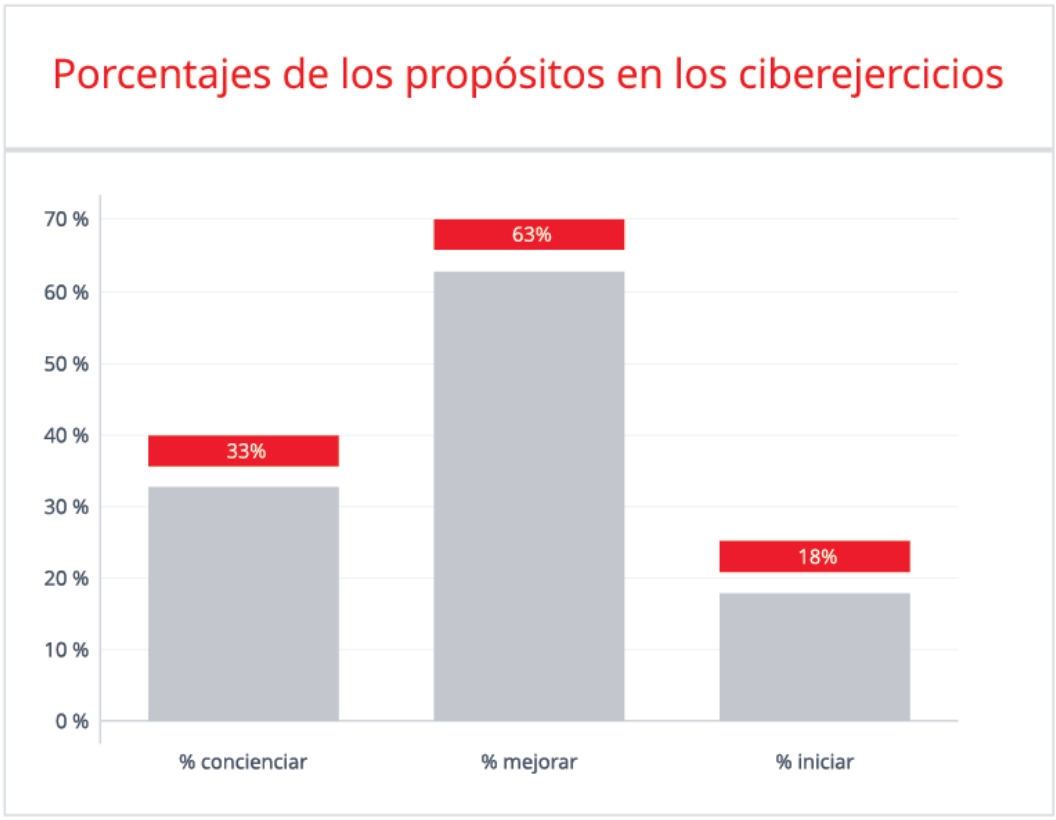

Figura 42. Porcentaje de aparición según el propósito de los ejercicios.

El ciberejercicio puede estar centrado en la fase previa al incidente, durante el incidente o después del incidente, pudiendo cubrir varias fases.

La siguiente figura muestra la aparición según la fase del incidente cubierta en los ciberejercicios realizados, pudiendo ser varias por ejercicio, y se ha representado la cobertura de todas las fases del incidente. El cómputo global de los porcentajes, por tanto, no tiene que corresponderse con 100.

Se ha comprobado que la principal área de actuación de los ejercicios corresponde a la respuesta ante incidentes, es decir, la fase durante el incidente es la que más aparece. También es destacable que si el ciberejercicio se realiza conjuntamente con un ejercicio de gestión de crisis, involucrando a los servicios de emergencia, la fase de después del incidente se suele abordar.

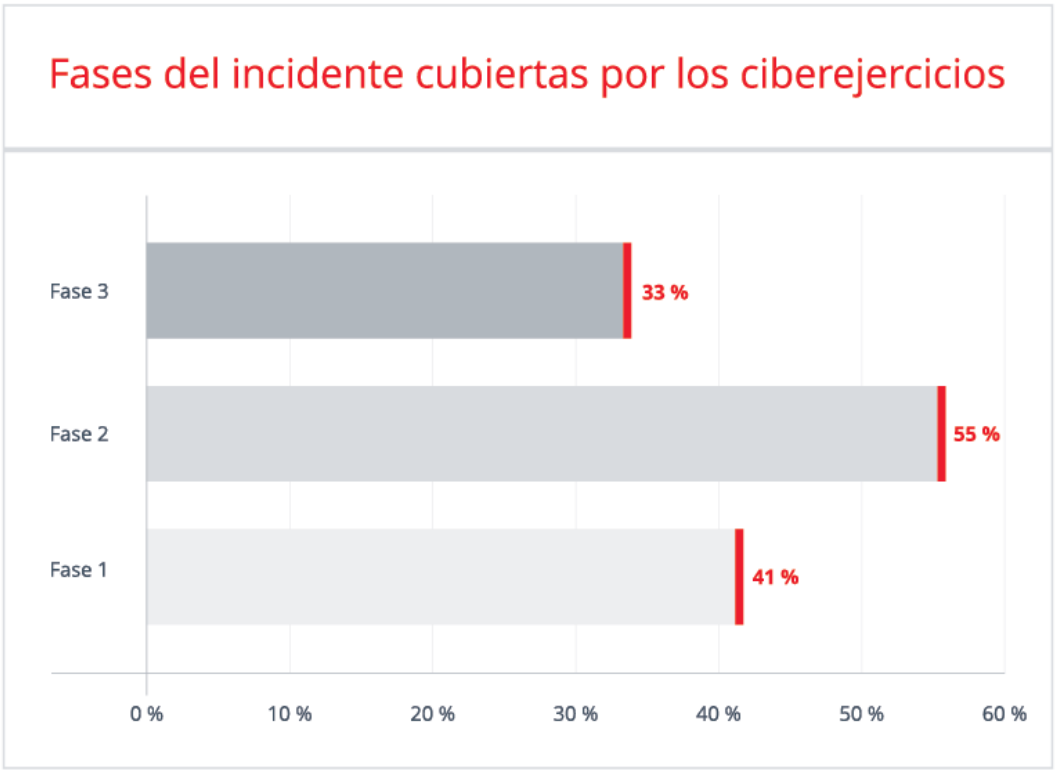

Figura 43. Porcentaje de aparición según las fases del incidente cubiertas por los ejercicios.

5.2.3 Situación en España

España ha participado en los distintos ciberejercicios que se han organizado en Europa con el impulso de la Comisión Europea y también en aquellos, como país aliado, que ha organizado la OTAN. Esto permite asegurar que la cooperación y coordinación de España con el resto de países de su entorno, ya sean por la parte Europea o por la parte de la alianza Atlántica está garantizada. La siguiente figura muestra el número de ciberejercicios en los que ha participado España.

Figura 44. Número de ciberejercicios participados por España.

En los ciberejercicios organizados por los EEUU (*Cyber Storm*) la participación de países europeos como Alemania, Holanda, Francia o el Reino Unido es habitual, pero España no ha participado en estos ejercicios transatlánticos.

Por otro lado, Alemania ha sido el único país miembro del grupo de CERTs gubernamentales Europeos (EGC) en participar en un ciberejercicio de la zona Asia-Pacífico organizado por la APCERT. España al ser miembro del EGC, podría participar en futuras ediciones de dichos ejercicios.

Desde una visión más local, España ha organizado varios ciberejercicios tanto en el ámbito militar como en el ámbito civil. Si bien, se detecta que los ciberejercicios enfocados por sectores verticales adolecen del modelo basado en operaciones, es de suponer que un futuro próximo se realizarán a pesar del enorme esfuerzo en recursos que es necesario emplear tanto en su preparación como en su ejecución, dados los resultados que se obtienen.

Por sectores verticales tratados en España, la única variación llamativa respecto a la totalidad de los ejercicios es la poca implicación del sector financiero en los mismos.

Siguiendo con el ámbito nacional, en España no se ha realizado un ejercicio conjunto de gestión de crisis integral que incluya también la parte cibernética, tal y como por

ejemplo ha realizado Alemania o la OTAN (pese a su pertenecía a OTAN, España no ha participado en estos ciberejercicios).

6 CONCLUSIONES

El impulso Europeo a través de la Agenda Digital para la realización de ciberejercicios, ha conseguido que la mayoría de los estados miembros participen en ciberejercicios pan-Europeos e incluso que realicen ciberejercicios en el ámbito nacional.

Se ha constatado que muchos países asumen la naturaleza global, compleja y cada vez más sofisticada de las amenazas en el ciberespacio, siendo necesario abordar estas amenazas en cooperación con otros países. En ese sentido se han dado casos de países europeos que:

1. Realizan de forma puntual un ejercicio nacional, aunque participan en los europeos.
2. Realizan ejercicios nacionales y europeos de forma independiente y sin coordinar la realización de unos con otros.
3. Pretenden sincronizar sus ejercicios nacionales con los europeos de forma que se realicen paralelamente.
4. Participan activamente en ejercicios de ámbito internacional, no sólo europeo.

Aunque inicialmente el sector público y el privado no participaban conjuntamente en ciberejercicios, actualmente se ha convertido en la práctica habitual, e incluso deseable. Si participa solamente el sector público, suele responder a la necesidad de iniciar o mejorar las capacidades nacionales relacionadas con la seguridad en el ciberespacio antes de involucrar al sector privado. También puede responder a que el ámbito del ejercicio se ciñe al entorno militar.

Se ha constatado la alta participación de los países Europeos en ciberejercicios de carácter internacional, estando alineado con la tendencia de que los ciberejercicios incrementen su grado de internacionalización, buscando incrementar el número de países participantes.

La mayor parte de los ciberejercicios realizados son de tipo *tabletop*, juegos o simulacros. Si bien es posible que muchos seminarios o talleres realizados no han sido contabilizados como ciberejercicios.

Aunque el objeto de la evaluación de un ejercicio puede considerar bastantes aspectos, los diferentes enfoques, tanto colectivos como individuales, han convivido sin fisuras en las distintas realizaciones.

Muchos ciberejercicios están estructurados para celebrarse en diferentes fases de ejecución, cada una orientada a un rol distinto dentro de cada organización. En este

sentido, se puede encontrar un hilo conductor en la realización de dichos ciberejercicios, pero también podrían ser considerados como ejercicios independientes.

La difusión que se da a los resultados de forma pública cada vez es más exigua, infiriéndose la difusión privada de los resultados a cada participante.

Si bien países como EEUU orientan sus ciberejercicios a cubrir todas las fases del incidente, se ha identificado la necesidad de cubrir la fase de recuperación en la planificación de nuevos ciberejercicios.

Gran parte de los ciberejercicios se realizan de forma periódica, con una regularidad anual o bianual. Esto permite validar las mejoras de los mismos, o la capacitación de los participantes. Por otra parte, la evolución de las amenazas y la tecnología dificulta esta capacidad de mejora, pues requiere evaluar otros aspectos.

Cada vez aparecen más ciberejercicios que involucran a nuevos sectores verticales, siendo los Estados Unidos el país pionero en organizar este tipo de ejercicios exclusivamente para un sector como puede ser el financiero o el de la salud. Constatándose de este modo la dependencia de dichos sectores verticales con las tecnologías de la información.

Respecto a los sectores verticales involucrados en los ciberejercicios se comprueba que:

- ✓ Existe una alta involucración de los sectores verticales de Transporte, Energía y TIC.
- ✓ Es habitual que se tenga en cuenta las interdependencias sectoriales existentes cuando coinciden varios sectores verticales en un mismo ciberejercicio.
- ✓ No hay constancia de ciberejercicios que involucren a los sectores I+D o Espacial.
- ✓ Existe la necesidad de impulsar el resto de sectores verticales.

Respecto a la situación en España se comprueba que:

- ✓ Existe cooperación y coordinación con el resto de países de su entorno, ya sean por la parte Europea o por la parte de la alianza Atlántica.
- ✓ Sería conveniente participar en ciberejercicios transatlánticos.
- ✓ Es necesario impulsar los ciberejercicios nacionales basados en operaciones.
- ✓ Menor implicación del sector financiero comparado con el resto de ciberejercicios realizados por otras naciones.

- ✓ Sería necesario realizar un ejercicio conjunto de gestión de crisis integral que incluya la parte cibernética.

7 INDICES y REFERENCIAS

7.1 Índice de figuras

7.2 Índice de tablas