



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA



Trabajo Fin de Master

Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en  
España dentro de un marco I+D+i.

Víctor E. Vera Pinto

Fernando González Ladrón de Guevara

Julio, 2017

Universidad Politécnica de Valencia

Facultad de Administración y Dirección de Empresas.

Master en Gestión de Empresas Productos y Servicios

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en*

*España dentro de un marco I+D+i*

Victor E. Vera Pinto

## **AGRADECIMIENTOS**

*A Dios por sobre todas las cosas.*

*A mis padres.*

*A mis hermanos.*

*A mi esposa.*

*A mi tutor.*

## **TABLA DE CONTENIDOS**

<b>AGRADECIMIENTOS .....</b>	<b>2</b>
<b>TABLA DE CONTENIDOS .....</b>	<b>3</b>
<b>RESUMEN.....</b>	<b>7</b>
<b>RESUM .....</b>	<b>8</b>
<b>ABSTRACT .....</b>	<b>9</b>
<b>INTRODUCCIÓN.....</b>	<b>10</b>
<b>1 PLANTEAMIENTO DEL PROBLEMA .....</b>	<b>13</b>
1.1 Formulación del problema. ....	13
1.2 Objetivos de la investigación .....	16
<i>Objetivo General .....</i>	<i>16</i>
<i>Objetivos específicos.....</i>	<i>16</i>
1.3 Justificación del estudio .....	17
1.4 Ámbito de la investigación .....	18
<b>2 MARCO TEÓRICO – CONCEPTUAL .....</b>	<b>20</b>
2.1 Antecedentes de la investigación .....	20
2.2 Estrategia nacional de ciberseguridad (ENC).....	24
2.3 Modelo de excelencia EFQM .....	27
2.4 Red de Excelencia Nacional de Investigación en Ciberseguridad. ....	34
2.5 Conceptos fundamentales de la excelencia .....	37
2.6 Proceso de autoevaluación en modelo de excelencia EFQM.....	42
2.7 Quick Self-Assessment del modelo de excelencia EFQM.....	45
<b>3 MARCO METODOLÓGICO.....</b>	<b>48</b>
3.1 Tipo de investigación.....	49
3.2 Diseño de la investigación .....	50
3.3 Población y muestra.....	50
3.4 Técnica e instrumento de recolección de datos.....	51

<i>Cuestionario orientado a determinar la necesidad de un modelo parcial de excelencia EFQM para desarrollo del ecosistema de ciberseguridad en España dentro del marco I+D+i</i> .....	52
<i>Entrevista a experto</i> .....	54
3.5 Validez y confiabilidad del instrumento .....	55
<b>4 RESULTADOS DE LA INVESTIGACIÓN</b> .....	<b>56</b>
4.1 Cuestionario orientado a determinar la necesidad de un modelo parcial de excelencia EFQM para desarrollo del ecosistema de ciberseguridad en España dentro del marco I+D+i. ....	56
<i>Análisis de resultados</i> .....	56
<i>Discusión de los resultados</i> .....	58
4.2 Entrevista a experto.....	60
<i>Análisis de resultados</i> .....	61
<i>Discusión de los resultados</i> .....	68
4.3 Conclusiones .....	72
4.4 Modelo parcial de excelencia EFQM para la ciberseguridad en España dentro del marco I+D+i.	74
<i>Metodología de intervención</i> :.....	75
<i>Interpretación del Modelo parcial desde la perspectiva de la ciberseguridad en España dentro del marco I+D+i.</i>	79
<i>Proceso de autoevaluación (Formularios con reuniones de trabajo)</i> .....	92
<i>Proceso de planes de acción para la mejora</i> .....	105
4.5 Recomendaciones .....	109
<b>ANEXOS</b> .....	<b>111</b>
<b>BIBLIOGRAFIA</b> .....	<b>137</b>

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en  
España dentro de un marco I+D+i*

Victor E. Vera Pinto

ÍNDICE DE TABLAS

Tabla 1. DAFO del ecosistema español de ciberseguridad dentro de marco I+D+i. Fuente: INCIBE (2015).....	26
Tabla 2. Relación de los criterios de los facilitadores del modelo EFQM con el diagnóstico de ciberseguridad en España dentro del marco I+D+i. Fuente: Elaboración propia.....	32
Tabla 3. Expectativa de criterio facilitador por objetivo estratégico del RENIC. Fuente: Elaboración propia. ....	40
Tabla 4. Expectativa de criterio facilitador por objetivo estratégico del RENIC (Cont.). Fuente: Elaboración propia. ....	41
Tabla 5. Percepción y desempeño en agencias de innovación bajo el modelo EFQM. Fuente: (EFQM, 2012).....	44
Tabla 6. Respuestas de aplicación de cuestionario. Fuente: Elaboración propia. ....	57
Tabla 7. Hoja REDER Criterio facilitadores. Fuente: Moreno (2007). ....	83
Tabla 8. Hoja REDER Criterios resultados. Fuente: Moreno (2007). ....	84
Tabla 9. Modelo de formulario de subcriterio facilitadores. Fuente: Moreno (2007).....	94
Tabla 10. Modelo de formulario de subcriterio resultados. Fuente: Moreno (2007). ....	95
Tabla 11. Metodología de calculo de puntuaciones para criterios facilitadores. Fuente: Moreno (2007).104	
Tabla 12. Metodología de cálculo de puntuaciones para criterios resultados. Fuente: Moreno (2007)....	104
Tabla 13. Calculo de puntuación total. Fuente: Moreno (2007). ....	104
Tabla 14. Modelo de tabla de puntuación de acciones de mejora. Fuente: Elaboración propia. ....	107
Tabla 15. Modelo de calendario de implantación de acciones de mejora. Fuente: Elaboración propia. ..	107
Tabla 16. Modelo de tabla para control de ejecución de acciones de mejora. Fuente: Elaboración propia, .....	108
Tabla 17. Relación de antecedentes de la investigación revisados. ....	114
Tabla 18. Resultados de cuestionario - <i>Sustaining outstanding results</i> . Fuente Elaboración propia.....	123
Tabla 19. Resultados de cuestionario - <i>Adding value for costumers</i> . Fuente Elaboración propia .....	124
Tabla 20. Resultados de cuestionario - <i>Developing organizational capacity</i> . Fuente Elaboración propia .....	125
Tabla 21. Resultados de cuestionario - <i>Managing with agility</i> . Fuente Elaboración propia.....	126
Tabla 22. Resultados de cuestionario - <i>Leading with vision, inspiration and integrity</i> . Fuente Elaboración propia .....	127
Tabla 23. Resultados de cuestionario - <i>Succeeding through the talent of people</i> . Fuente: Elaboración propia .....	128
Tabla 24. Resultados de cuestionario - <i>Harnessing creativity and innovation</i> . Fuente Elaboración propia .....	129
Tabla 25. Resultados de cuestionario - <i>Creating a sustainable future</i> . Fuente Elaboración propia .....	130

## ÍNDICE DE ILUSTRACIONES

Ilustración 1. Síntesis de área de aportación de investigaciones consultadas. Fuente: Elaboración propia. ....	23
Ilustración 2. Modelo de excelencia EFQM. Fuente: Trott, 2009. ....	28
Ilustración 3. Conceptos fundamentales EFQM de la excelencia. Fuente: EFQM (2012). ....	37
Ilustración 4. Self-Assessment en Modelo de excelencia EFQM. Fuente Elaboración Propia.....	43
Ilustración 5. Estructura del Quick Self-Assessment. Fuente: Elaboración propia. ....	45
Ilustración 6. Alcances (Tipo de investigación). Fuente: Elaboración propia. ....	49
Ilustración 7. Diagrama de metodología de intervención. Fuente: Moreno (2007). ....	76
Ilustración 8. Rueda de la gestión de la calidad. Fuente: EFQM (2012). ....	81
Ilustración 9. Criterios y subcriterios de modelo EFQM. Fuente: Elaboración propia.....	87
Ilustración 10. Causas de relación de subcriterios con eje “comunicación interna”. Fuente: Elaboración propia. ....	91
Ilustración 11. Resumen de proceso de planes de acción. Fuente: Elaboración propia. ....	106

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en  
España dentro de un marco I+D+i*

Victor E. Vera Pinto

## **RESUMEN**

El objetivo principal de la investigación fue generar un Modelo Parcial de Excelencia EFQM para la ciberseguridad en España dentro del marco I+D+i. Fundamentado en los aportes teóricos de: Dalkir (2005), Moreno (2007), Trott (2009), EFQM (2012), INCIBE (2015) y Vinnakota (2016). Metodológicamente, la investigación se enmarcó en un enfoque mixto, donde a través de un estudio cuantitativo se incluyeron las siguientes fases: planteamiento de un problema de estudio delimitado y concreto, revisión de antecedentes asociados y relevantes al problema, construcción del marco teórico basado en una revisión literaria, elaboración de varias hipótesis, recolección de datos de los participantes que se estudian y análisis de la información obtenida. Para el proceso de recolección de información se emplearon dos instrumentos: un cuestionario dirigido al sector académico de tipo Likert conformado por 20 items, que contaba con cinco opciones de respuesta y una entrevista semi-estructurada dirigida a un experto en ciberseguridad e I+D+i. Ambas, empleadas para lograr los objetivos específicos y a su vez, determinar la necesidad de un SGC (Sistema para la Gestión de la Calidad) en el funcionamiento del ecosistema de ciberseguridad en España, liderado por el RENIC (Red de Excelencia Nacional de Investigación en Ciberseguridad). El análisis de los datos obtenidos se desarrolló a través de un enfoque cualitativo, donde se establecieron y desarrollaron las acciones para obtener la información, basados en el *Quick Self-assessment* propuesto por EFQM (2012). Seguidamente, se efectuó un estudio cualitativo de la información proveniente del cuestionario y de la entrevista, contrastando las opiniones de los agentes, considerando la tipología a la cual pertenecen en el ecosistema de ciberseguridad español y analizando las convergencias y divergencias evidenciadas al evaluar el desempeño del RENIC, a través de la consideración de los atributos de la excelencia definidos en el modelo EFQM. Esta estrategia ha permitido orientar el diagnóstico del proceso para obtener como resultado la elaboración de la propuesta. Finalmente, y en base a los resultados arrojados por la investigación se diseñó una propuesta del Modelo Parcial de Excelencia EFQM para la ciberseguridad en España dentro del marco I+D+i.

Palabras Clave: Ciberseguridad, Gobernanza, Innovación, Colaboración, Seguridad de la Información

## **RESUM**

L'objectiu principal de la investigació va ser generar un Model Parcial d'Excel·lència EFQM per a la ciberseguridad a Espanya dins del marc I+D+i. Fonamentat en les aportacions teòriques de: Dalkir (2005), Moreno (2007), Trott (2009), EFQM (2012), INCIBE (2015) i Vinnakota (2016). Metodològicament, la investigació es va emmarcar en un enfocament mixt, on a través d'un estudi quantitatiu es van incloure les fases següents: plantejament d'un problema d'estudi delimitat i concret, revisió d'antecedents associats i rellevants al problema, construcció del marc teòric basat en una revisió literària, elaboració de diverses hipòtesis, recollida de dades dels participants que s'estudien i anàlisi de la informació obtinguda. Per al procés de recollida d'informació es van emprar dos instruments: un qüestionari dirigit al sector acadèmic de tipus Likert conformat per 20 ítems, que comptava amb cinc opcions de resposta i una entrevista semi-estructurada dirigida a un expert en ciberseguridad i I+D+i. Ambdós, emprades per a aconseguir els objectius específics i al seu torn, determinar la necessitat d'un SGC (Sistema per a la Gestió de la Qualitat) en el funcionament de l'ecosistema de ciberseguridad a Espanya, liderat pel RENIC (Xarxa d'Excel·lència Nacional d'Investigació en Ciberseguridad). L'anàlisi de les dades obtinguts es va desenrotllar a través d'un enfocament qualitatiu, on es van establir i van desenrotllar les accions per a obtenir la informació, basats en el Quick Self-assessment proposat per EFQM (2012). A continuació, es va efectuar un estudi qualitatiu de la informació provinent del qüestionari i de l'entrevista, contrastant les opinions dels agents, considerant la tipologia a la qual pertanyen en l'ecosistema de ciberseguridad espanyol i analitzant les convergències i divergències evidenciades a l'avaluar l'exercici del RENIC, a través de la consideració dels atributs de l'excel·lència definits en el model EFQM. Esta estratègia ha permès orientar el diagnòstic del procés per a obtenir com resultat l'elaboració de la proposta. Finalment, i basant-se en els resultats intrèpids per la investigació es va dissenyar una proposta del Model Parcial d'Excel·lència EFQM per a la ciberseguridad a Espanya dins del marc I+D+i.

Paraules Clau: Ciberseguridad, Governança, Innovació, Col·laboració, Seguretat de la Informació.

## **ABSTRACT**

The main objective of the research was to generate an EFQM Partial Excellence Model for cybersecurity in Spain within the R & D framework. Based on theoretical contributions of Dalkir (2005), Moreno (2007), Trott (2009), EFQM (2012), INCIBE (2015) and Vinnakota (2016). Methodologically, the research was a mixt framed where a quantitative approach was performed as the following steps: approaching a problem of delimited and concrete study, review of associated antecedents and relevant to the problem, construction of the theoretical framework based on a literary revision, elaboration of hypothesis, data collection of the participants being studied and analysis of the information obtained. For the data collection process, two instruments were used: a Likert type questionnaire addressed to the academic sector, that contains 20 items, which had 5 response options. Similarly, a semi-structured interview addressed to an expert in cybersecurity and R & D was applied to give answers to the specific objectives and to determine the necessity of a total quality management system (TQMS) to the functionality of the cybersecurity ecosystem in Spain, led by the RENIC (National Excellence Network in Cybersecurity Research). The analysis of the data obtained was developed through a qualitative approach, where the actions to obtain the information were established and developed, based on the Quick Self-assessment proposed by EFQM (2012). Then, a qualitative study of the information from the questionnaire and the interview was carried out, comparing the opinions of the agents according to the typology they represent in the ecosystem and analyzing the convergence and divergence evidenced in the evaluation of the performance of the RENIC, through the consideration of the excellence attributes defined in the EFQM model. This strategy has guided the process to obtain as a result the preparation of the proposal. Finally, and based on the results of the research, the EFQM Partial Excellence Model for cybersecurity in Spain was designed within the R & D framework.

Keywords: Cyber security, Governance, Innovation, Knowledge Sharing, Information Security.

## **INTRODUCCIÓN**

La ciberseguridad es un área de conocimiento que lleva arraigada en su piedra fundacional la evolución acelerada y continua, esto obedece a la gran cantidad de vulnerabilidades existentes en los sistemas de información, además de la velocidad evolutiva de las capacidades de los ciberatacantes y el contexto propuesto por las TIC en su acelerado proceso de desarrollo constante, por lo que la necesidad de mantenerse a la vanguardia resulta imperiosa ante los riesgos que representa el no hacerlo. En este sentido, la innovación, desarrollo e investigación (I+D+i) representa el camino en el que deberá buscar superar estos y los próximos retos a venir. Es por esto importante asumir la relevancia del R&D en la ciberseguridad y la necesidad de liderar hacia la excelencia todos los procesos I+D+i.

Ante esta realidad, España en 2016 propuso al RENIC como una solución que no solo se presenta como un canal para orientar los proyectos I+D+i, también busca incidir sobre otros grandes retos presentes en el ecosistema como lo son la falta de liderazgo y de integración entre sus agentes, la necesidad de mayor promoción y desarrollo nacional e internacional de los involucrados en el ecosistema y la carencia de profesionales especializados presentes en el sector. Tales retos, le exigen contar con modelos de gestión que logre coordinar las acciones de todos los agentes involucrados, porque será solo a través de la integración de la red que se podrán dar los pasos en la dirección correcta en este contexto tan dinámico y cambiante.

Esta investigación propone un modelo de gestión de calidad total que permite al RENIC contar con las herramientas y metodologías orientadas a la excelencia, necesarias para llevar al

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

éxito los macro objetivos estratégicos que se plantea. Bajo estos parámetros, resulta oportuno determinar si la necesidad de implantación de dicho modelo existe, por lo que basado en la metodología propuesta por EFQM (2012), se buscó determinar la postura en este asunto de algunos agentes pertenecientes al ecosistema.

En este sentido, se desarrolló un trabajo que se estructuró de cuatro capítulos donde en el primero de ellos (Planteamiento del problema) se busca describir el contexto actual de ciberseguridad, haciendo hincapié en la actual necesidad de desarrollo e integración en I+D+i a nivel nacional ante la acelerada evolución de las TIC.

Seguidamente, se presenta el segundo capítulo (Marco teórico-conceptual) en el que se delimita el alcance del problema en estudio. Esto se evidencia por medio de la contextualización del panorama actual de ciberseguridad en España, a través de la revisión sistemática de investigaciones publicadas por agentes relevantes del ecosistema de ciberseguridad español, además de publicaciones académicas y reportes emitidos por entes públicos nacionales e internacionales. Analizando de estos antecedentes la información relevante del contexto en estudio y detectando necesidades de mejora en la gobernanza nacional del ecosistema de ciberseguridad en España. Así mismo, se desarrolla el sustento teórico que plantea el modelo de excelencia EFQM y la posición del RENIC (Red de Excelencia Nacional de Investigación en Ciberseguridad) dentro del ecosistema.

El tercer capítulo, referido al desarrollo del marco metodológico, contempla la metodología empleada para el desarrollo de esta investigación, específicamente el tipo y el diseño de la investigación, las técnicas e instrumentos de recolección de datos empleados, la validez y la

confiabilidad son descritos en este apartado. Finalmente, en el ultimo capitulo (Resultados de la investigación) se presentan los resultados obtenidos del estudio realizado incluyendo una propuesta base para el desarrollo del modelo parcial de excelencia EFQM para la ciberseguridad en España dentro del marco I+D+i.

Ante este contexto, donde las brechas tecnológicas entre países se hacen cada día más pronunciadas y los ciberataques han pasado a ser armas de guerra entre gobiernos, resulta imperioso este tipo de iniciativas de investigación, ya que solo a través de la capacidad de administrar los recursos se logrará superar los retos actuales y venideros en la ciberseguridad española.

## **1 PLANTEAMIENTO DEL PROBLEMA**

---

### **1.1 Formulación del problema.**

España en el 2013 a través del Consejo de Seguridad Nacional promovió la creación de una Estrategia de Ciberseguridad Nacional (ECN), al amparo de la Estrategia de Seguridad Nacional aprobada por el Consejo de Ministros (Presidencia del Gobierno, 2013), la cual tiene como fin el establecer las directrices generales del uso seguro del ciberespacio. Este documento oficial esta disgregado en 5 capítulos donde se establecen los principios rectores, los objetivos y las líneas de acción de la ciberseguridad, así como su implicación en el Sistema de Seguridad Nacional. La ECN de España fija las directrices en el uso seguro del ciberespacio, promoviendo una visión integradora en temas como la innovación y la gestión del conocimiento, buscando garantizar seguridad y progreso a través de la coordinación y cooperación de todas las administraciones públicas entre ellas, con el sector privado y con los ciudadanos.

Cabe destacar que la innovación y la gestión del conocimiento son premisas comunes en las estrategias nacionales de ciberseguridad de varios países, en algunos de manera más explícita como es en los casos de Alemania y Japón, en los cuales sus ECN establecen la necesidad de alinear las acciones de investigación, desarrollo e innovación (I+D+i) de las funcionalidades de las tecnologías de la información y la comunicación (TIC) con las necesidades que representan las amenazas que involucran el uso del ciberespacio (Luijff, Besseling, & De Graaf, 2013). Con base en lo expuesto, se debe considerar el I+D+i, parte esencial de las líneas de acción de una estrategia de ciberseguridad, ya que la evolución constante de las amenazas y la posibilidad de sufrir la

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

explotación de una vulnerabilidad requieren de respuestas y soluciones innovadoras y vanguardistas (UK-Cabinet-Office, 2011)

En este sentido, España además de considerar el I+D+i en su ECN, promueve acciones de investigación, desarrollo e innovación a distintos niveles de la administración pública, destacándose en el área de ciberseguridad las acciones promovidas por el Polo tecnológico de ciberseguridad en España, el Instituto nacional de ciberseguridad (INCIBE), el Centro Criptológico Nacional (CCN) y la Red de excelencia nacional de investigación en ciberseguridad (RENIC). Cada institución evidencia acciones que buscan promover el desarrollo del sector, pero este ecosistema deberá resolver diversos retos y limitaciones para abordar la mejora de su competitividad y resultados. Estos retos, de profundo calado e impacto, constituyen una oportunidad y justifican la necesidad de proponer un modelo de excelencia EFQM que estimule la conexión y la puesta en común de los agentes presentes en el ecosistema de innovación nacional para así dar respuesta a la actual desarticulación (INCIBE, 2015).

Lo anteriormente expuesto sobre la relevancia del I+D+i en la ciberseguridad, es una realidad asumida por la mayoría de las empresas de ciberseguridad en España, ya que de acuerdo a datos del Observatorio Nacional de las telecomunicaciones y de la SI (ONTSI), para el 2014 estaban registradas 533 organizaciones y estas contaron con una facturación cercana a los 600 millones de euros, en donde la inversión en ciberseguridad por parte de las organizaciones de servicios TIC del sector era de 78 millones, representando esto el 98,5 % del total de la inversión del sector. Este conjunto de organizaciones se compone en pequeña parte por multinacionales y fundamentalmente por pymes y microempresas, habiendo demostrado este último tipo de

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

organizaciones mayor facilidad para la explotación de áreas de desarrollo de innovaciones, propiciando la conformación de un “cluster” de organizaciones que sirve de fuente de colaboración e innovación para el sector (INCIBE 2016).

Así mismo, el sector ha evidenciado intenciones de integración, quedando claro en acciones como la conformación del Polo Tecnológico de Ciberseguridad de España, el cual ha estado más orientado a la integración en acciones de internacionalización y de mejoramiento del posicionamiento de la industria española en ciberseguridad, no manifestando acciones trascendentales en el área de I+D+i (Polo Tecnológico Nacional Ciberseguridad, 2016). En este orden de ideas, ante la falta de integración en los proyectos y la poca evidencia de acciones innovadoras que promuevan la percepción internacional de la industria, el Instituto Nacional de Ciberseguridad (INCIBE) presenta un análisis detallado del contexto nacional, ante el cual propone acciones concretas como lo son la instauración de una Red de centros de excelencia en I+D+i en ciberseguridad (INCIBE, 2015).

En este estudio de viabilidad, oportunidad y diseño de una red de centros de excelencia en I+D+i en ciberseguridad, el INCIBE dibuja el contexto nacional de ciberseguridad, contando para su desarrollo con la colaboración de diversos agentes representativos pertenecientes a las cuatro grandes tipologías de entidades que conforman cualquier ecosistema de este tipo: administración pública, sector académico, organizaciones de soporte a la I+D+i y el sector industria (INCIBE, 2015). Evidenciando en sus resultados claras carencias en el desarrollo del sector, conllevando esta apreciación a la constitución en julio del 2016 como entidad jurídica de la Red de excelencia

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

nacional de investigación en ciberseguridad (RENIC) así como su misión, visión, valores y objetivos.

Ante el panorama actual, es necesario establecer las acciones específicas que deberán ejecutar los distintos elementos que conforman el ecosistema de la ciberseguridad en España dentro del marco I+D+i y es a través de la implantación de un modelo de excelencia basado en las metodologías propuestas por la Fundación Europea para la Gestión de la Calidad (European Foundation Quality Management) para organizaciones de innovación, que la ciberseguridad española podrá dar los primeros pasos para su distinción internacional así como en la innovación en sus productos y servicios.

Considerando lo antes expuesto cabe preguntarse: ¿qué características tendrá un modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro del marco I+D+i?

## **1.2 Objetivos de la investigación**

### **Objetivo General**

Proponer un modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro del marco I+D+i.

### **Objetivos específicos**

- Identificar la necesidad de un modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro del marco I+D+i.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

- Determinar si el RENIC cuenta con las facultades necesarias para liderar la implantación de un modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro del marco I+D+i.
- Establecer si el ecosistema actual de la ciberseguridad en España dentro del marco I+D+i cuenta con los requerimientos para la implantación del modelo parcial de excelencia EFQM.
- Diseñar un modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro del marco I+D+i.

### **1.3 Justificación del estudio**

Dentro de esta investigación se relacionan dos disciplinas, la innovación y la ciberseguridad, las cuales deberán unificar posturas para aportar respuestas que logren mitigar el contexto actual en materia de riesgos y amenazas que representa el uso del ciberespacio, considerando las capacidades actuales de los sistemas TIC y sus tendencias. La dupla enmarcada dentro de esta investigación estará presente en cada uno de los apartados, intentando que los campos puedan desarrollarse de manera coherente sin el dominio de uno sobre el otro y engranándose en perfecto funcionamiento para conseguir los fines del proyecto.

Ahora bien, la naturaleza de la ciberseguridad reclama bases donde sustentar con pertinencia y claridad, la concepción y el desarrollo de nuevos procedimientos de innovación. A eso, no escapa la necesidad del establecimiento de perfiles profesionales para la rama acordes a las necesidades del mercado y la incorporación de un sistema de certificación profesional para el sector, que enaltezca la ciberseguridad española en el ámbito internacional. Es por ello que el

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

requisito del modelo de excelencia EFQM es una condición necesaria pero no suficiente cuando de I+D+i se trata.

Así mismo, la necesidad de crear un modelo de excelencia EFQM que disipe las dudas y derrumbe los obstáculos que por diferentes razones se han interpuesto entre el “deber ser” y el “ser” de la práctica de procedimientos innovadores del profesional de la ciberseguridad, representa no sólo un motivo, sino que justifican plenamente el desarrollo de una investigación. Es por esto, que la importancia de la investigación radica en encontrar una interacción perfectamente aprovechable entre los elementos del ecosistema actual de la ciberseguridad de España, y la innovación como la base didáctica, educativamente pertinente y tecnológicamente viable para el desarrollo de competencias dentro del RENIC.

Así mismo, teóricamente será un aporte a la divulgación, clarificación y unificación de criterios en cuanto a los contenidos del área específica de la gestión de la innovación de procedimientos, proporcionado de una manera práctica una herramienta para la solución de un problema común dentro del ámbito de la ciberseguridad. Además, es pertinente mencionar que el trabajo se justifica porque presenta una metodología sistemática y coherente para el proceso de investigación.

#### **1.4 Ámbito de la investigación**

La investigación se desarrolla dentro del programa de la Facultad de Administración y Dirección de Empresas de la Universidad Politécnica de Valencia, Maestría en Gestión de

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en  
España dentro de un marco I+D+i*

Victor E. Vera Pinto

Empresas, Productos y Servicios. En un lapso comprendido desde noviembre 2016 hasta julio 2017.

Así mismo, los contenidos teóricos se desarrollan considerando en primer lugar la gestión de la innovación basada en los autores Trott (2009) y Tidd (2005); y la gestión del conocimiento basado en los autores Dalkir (2005) y Lugen (2004). De igual manera, se delimita bajo los autores Hernández, Fernández y Baptista (2007) como una investigación orientada a un enfoque mixto descriptivo. Finalmente, se establece como delimitación geográfica de la investigación España.

## **2 MARCO TEÓRICO – CONCEPTUAL**

---

Este capítulo está compuesto por un resumen de la información obtenida de los antecedentes de la investigación. Seguidamente se sintetizarán las carencias presentes en el ecosistema de ciberseguridad en España dentro del marco I+D+i detectadas al considerar las fuentes consultadas. Posteriormente, se analizará el sustento teórico consultado del modelo de excelencia EFQM para así desarrollar el instrumento que permitirá determinar si existe la necesidad.

### **2.1 Antecedentes de la investigación**

Para el cumplimiento de los objetivos planteados se consultaron 51 investigaciones. Estas investigaciones fueron seleccionadas de búsquedas realizadas en las bases de datos Scopus, Web of Knowledge y Science Direct, siendo utilizadas como *search tag* las palabras: “*Innovation*”, “*cyber security*”, “*governance*”. A continuación son descritas en orden de la relevancia las 4 más influyentes en el desarrollo de este documento:

En primer lugar, se tiene la investigación realizada por el Instituto nacional de Ciberseguridad (INCIBE) en el 2015 titulada: “Estudio de viabilidad, oportunidad y diseño de una red de centros de excelencia en I+D+i”. Este trabajo supuso la participación de un gran número de representantes del sector y se considera de suma importancia para la elaboración del presente estudio por aportar:

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

- La definición de las tipologías de entidades que conforman el ecosistema de ciberseguridad dentro del marco I+D+i en España.
- El posicionamiento competitivo global del ecosistema de ciberseguridad español dentro del marco I+D+i.
- La modelización de la red de excelencia para la ciberseguridad en España dentro del marco I+D+i.
- La muestra considerada para dar respuesta al cuestionario desarrollado en esta investigación.

De igual manera, se presenta un segundo antecedente realizado en el 2016 por Vinnakota titulado: “A second order cybernetic model for governance of cybersecurity in Enterprises”. Esta investigación presenta los siguientes aportes de interés:

- Diagnostico de las necesidades de orden mundial en ciberseguridad en el marco de la gobernanza en las organizaciones.
- Modelo cibernético para la gobernanza de las organizaciones de ciberseguridad.

Un tercer antecedente considerado de gran valor para el desarrollo de esta investigación se refiere al trabajo realizado en el 2012 por EFQM (European Foundation of Quality Management) titulado “EFQM framework for innovation agencies”. Sus aportes son:

- Los criterios de éxito para las organizaciones de I+D+i y el mapeo en el Modelo de Excelencia EFQM.
- La guía de evaluación de requerimientos en organizaciones de I+D+i para la implementación del modelo de excelencia EFQM.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

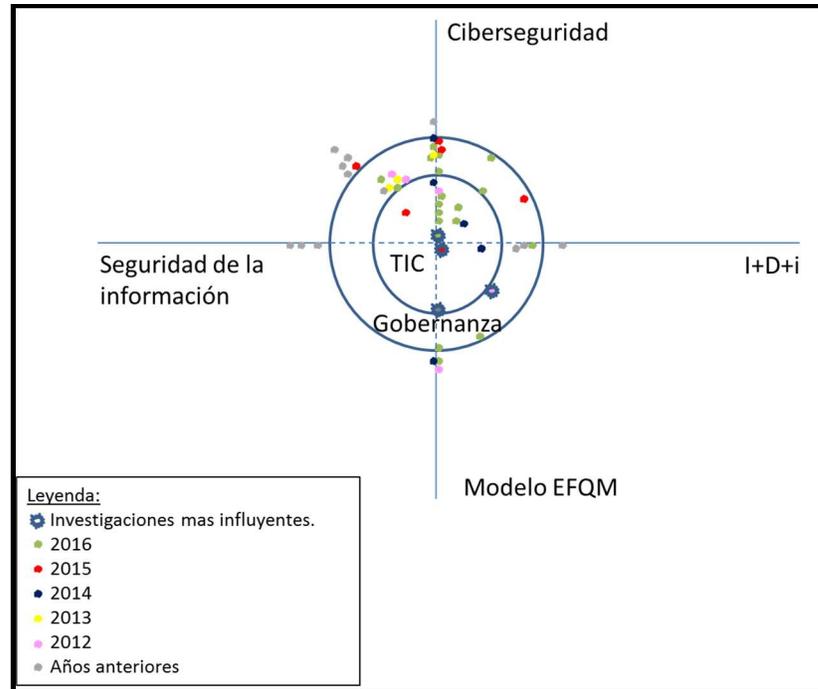
Victor E. Vera Pinto

- El “*Quick Self-assessment*”, autoevaluación para organizaciones I+D+i que permite determinar la madurez y el impacto de sus objetivos estratégicos en todos los agentes involucrados en la organización. A través de este instrumento también se puede detectar la necesidad del modelo de excelencia EFQM.

De igual forma Moreno (2007), brinda el cuarto antecedente titulado: “Guía para la aplicación del modelo EFQM de excelencia en entidades de acción social”, el cual aporta:

- Interpretación de los criterios y cuestiones transversales del modelo de excelencia EFQM.
- Métodos de intervención para la implantación de un modelo de excelencia EFQM.
- Hoja de puntuación REDER.
- Dificultades y problemáticas en la implantación de un sistema de gestión de la calidad.

Así mismo y con menor aportación a la investigación fueron consultados otros documentos (Ver anexo I) los cuales son categorizados en la ilustración 1 en función del área de contribución a esta investigación:



**Ilustración 1. Síntesis de área de aportación de investigaciones consultadas. Fuente: Elaboración propia.**

Es evidente en la ilustración 1, el gran número de investigaciones de gobernanza de ciberseguridad en las que se considera las TIC y sus tendencias antes descritas, pero pocas reflejan la importancia del I+D+i en la ciberseguridad (Hernandez-Munoz, Torane, & Amini, 2015; INCIBE, 2015; Kraemer-Mbula, Tang, & Rush, 2013; UK-Cabinet-Office, 2011) y mucho menos consideran algún sistema de gestión de calidad. Excluidos de esta tendencia, se presentan las investigaciones realizadas por el departamento de defensa de los Estados Unidos y UK Cabinet, siendo la consideración de un sistema de gestión de la calidad uno de los elementos que ha permitido a Estados Unidos y al Reino Unido contar con una posición privilegiada en materia de estrategias nacionales de ciberseguridad (Leiva, 2015; Luiijf et al., 2013).

## **2.2 Estrategia nacional de ciberseguridad (ENC).**

Desde una perspectiva más focalizada a la geografía considerada en este estudio, la ENC se presenta como el documento que fundamenta al gobierno para el desarrollo de las previsiones de seguridad nacional en lo relativo a la protección del ciberespacio y la implantación de forma coherente y estructurada de acciones para la prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas. En este documento, las TIC son consideradas en el primer objetivo específico el cual enuncia “garantizar que los sistemas TIC utilizados por las administraciones públicas posean el adecuado nivel de seguridad y resiliencia”. De igual forma, en lo concerniente al R&D se puede señalar la Sexta línea de acción, denominada “Conocimiento, competencias e I+D+i”, en la cual se busca promover la capacitación profesional, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad (Presidencia del Gobierno de España, 2013).

Del objetivo específico mencionado se han generado diversas acciones que han llevado al Centro Criptológico Nacional (CCN) a cumplir un rol neurálgico dentro de la seguridad de la información y la ciberseguridad de la administración pública (AAPP) (CCN, 2016; Cendoya, 2016; INCIBE, 2016). De forma muy distinta, se puede reseñar el desarrollo de la línea acción señalada de la ECN, evidenciándose una lenta evolución y con diversos factores limitantes, tanto generales como específicos, que han impactado de forma negativa en el funcionamiento del ecosistema I+D+i (INCIBE, 2015, 2016; ONTSI, 2016; Polo Tecnológico Nacional Ciberseguridad, 2016).

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

La diversidad de problemas suscitados en el desarrollo del I+D+i de ciberseguridad en España, van más allá de la falta de sistema de calidad eficiente ya que considera limitantes de ámbito general, estructural, además de las propias del contexto de la ciberseguridad. A partir de estos hallazgos, el Instituto Nacional de Ciberseguridad (2015) desarrolló el siguiente análisis DAFO:

AMENAZAS



**1. Competencia.**

1A. Países líderes con fuerte inversión a largo plazo en I+D+i y con políticas y focos de investigación claros, que sitúan comparativamente a España en la cola de la apuesta a largo plazo por la ciberseguridad.

**2. Mercado doméstico** limitado por la ausencia de tracción de la administración en la demanda temprana de soluciones punteras y la escasa demanda de soluciones por parte de los ciudadanos y empresas.

**3. Ciencia y conocimiento.**

3A. Limitaciones del sistema de ciencia y tecnología en el desarrollo e impulso del personal investigador.

3B. Enfoques de investigación con cierto continuismo y limitaciones de adaptación a los cambios, que limita el aprovechamiento de los nichos de oportunidad en ciberseguridad.

3C. Escasos impulsos en los incentivos al personal investigador para la transferencia de la investigación al mercado.

**4. Talento**

4A. Mayor atractivo de los países líderes, que aceleran el proceso de fuga de talento en España.

OPORTUNIDADES



**1. Contexto estratégico.**

1A. Ciberseguridad como asunto clave en las agendas gubernamentales

1B. Contexto normativo incipiente, con amplias oportunidades de catalizar la demanda de soluciones de ciberseguridad (delimitación de obligaciones y requisitos técnicos que deberán ser de obligado cumplimiento).

**2. Contexto financiero.**

2A. Aprovechamiento del entorno europeo como trampolín para incrementar la excelencia.

**3. Mercado.**

3A. Ciberseguridad como sector emergente, dinámico y en crecimiento, con grandes potenciales de crecimiento en los próximos años.

3B. Grandes oportunidades en la comercialización de soluciones en Latinoamérica.

3C. Identificación de sectores que puedan actuar como grandes tractores de I+D+i (early adopters), con grandes necesidades de soluciones de ciberseguridad y con capacidad de exportar estas soluciones al ámbito internacional.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

DEBILIDADES	D A F O
<p><b>1. Contexto estratégico.</b> 1A. Falta de concreción / operativización de las políticas públicas en ciberseguridad. 1B. Ausencia de focos y planes específicos para la I+D+i en ciberseguridad.</p> <p><b>2. Contexto financiero.</b> 2A. Baja conciencia y sensibilización de la sociedad (ciudadanía empresas y administración) sobre la importancia de la ciberseguridad. 2B. Cultura de aversión al riesgo que traduce bajos niveles de start ups y empresas de base tecnológica en ciberseguridad.</p> <p><b>3. Industria.</b> 3A. Escasa actividad de I+D en el ámbito empresarial.</p> <p><b>4. Ciencia y conocimiento.</b> 4A. Ausencia de liderazgo / débil posicionamiento internacional en materia de I+D+i en ciberseguridad del sector académico y de la industria. 4B. Múltiples focos en la actividad investigadora del sector académico sin que existan grupos de referencia o líderes en ninguna materia. 4C. Ecosistema amplio, diverso, fragmentado y desconectado sin unas dinámicas claras de relación entre sus agentes. 4D. Ecosistema por debajo de sus capacidades, debido al desaprovechamiento de las sinergias que un ecosistema de este volumen presenta a través de la colaboración</p> <p><b>5. Transferencia.</b> 5A. Tradicional desconexión ciencia-empresa. 5B. Los organismos de soporte a la innovación presentan disfuncionalidades en el proceso de transferencia tecnológica.</p> <p><b>6. Talento.</b> 6A. Proceso de fuga de talento hacia otras localizaciones mas atractivas económica y profesionalmente. 6B. Bajos niveles de retención y desarrollo de talento. 6C. Procesos de formación y capacitación que no están totalmente alineados con las necesidades del mercado</p>	
FORTALEZAS	D A F O
<p><b>1. Ciencia y conocimiento</b> 1A. Sector académico con masa crítica y capacidades investigadoras amplias y demostradas. Amplio margen de recorrido para la exploración y puesta en valor de las capacidades investigadoras en el ámbito de la ciberseguridad.</p> <p><b>2. Talento</b> 2A. Cierta nivel en el talento profesional e investigador, que presenta oportunidades para su retención, explotación y puesta en valor.</p> <p><b>3. Agentes del ecosistema de I+D+i</b> 3A. Excelente predisposición de agentes del ecosistema para impulsar la ciberseguridad.</p>	

Tabla 1. DAFO del ecosistema español de ciberseguridad dentro de marco I+D+i. Fuente: INCIBE (2015).

Esta información a pesar de ser muy valiosa para la investigación, no refleja en su totalidad el funcionamiento que actualmente del ecosistema de ciberseguridad en España dentro del marco

I+D+i, provocado en gran medida por la instauración en 2016 de la Red de excelencia nacional de investigación en ciberseguridad (RENIC), por ser éste un elemento que aspira grandes responsabilidades en el funcionamiento de dicho ecosistema (RENIC, 2016. Presentación del RENIC a la industria de ciberseguridad. Recuperado de <http://www.renic.es/es/index.html>). De igual manera, es necesario el desarrollo del sustento teórico del modelo EFQM de excelencia que permita determinar si las necesidades del ecosistema justifican la implantación de este sistema de calidad.

### **2.3 Modelo de excelencia EFQM**

El modelo de excelencia EFQM es presentado en 1999 por la Fundación Europea para la Gestión de la Calidad, la cual es una fundación conformada por 14 empresas líderes del occidente de Europa que tiene como misión el premiar a las organizaciones por la implantación eficiente de sistemas TQM (Total Quality Management). Este modelo reflejaba un mayor entendimiento y énfasis en el enfoque de cliente (y de mercado) orientando a los resultados. La idea subyacente es que los resultados (personas, clientes, sociedad y desempeño clave) se logran a través de un número de facilitadores para administrar y controlar los procesos de transformación de entrada / salida involucrados (Trott, 2009). En este sentido, el desempeño de la organización se mide por la autoevaluación, siendo definida ésta por el modelo como una revisión integral, sistemática y regular de las actividades de una organización y sus resultados, contrastándolos con un modelo de excelencia empresarial involucrando la innovación y el desempeño (Calvo-Mora et al., 2016).

Lo antes descrito es representado gráficamente de la siguiente manera:

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

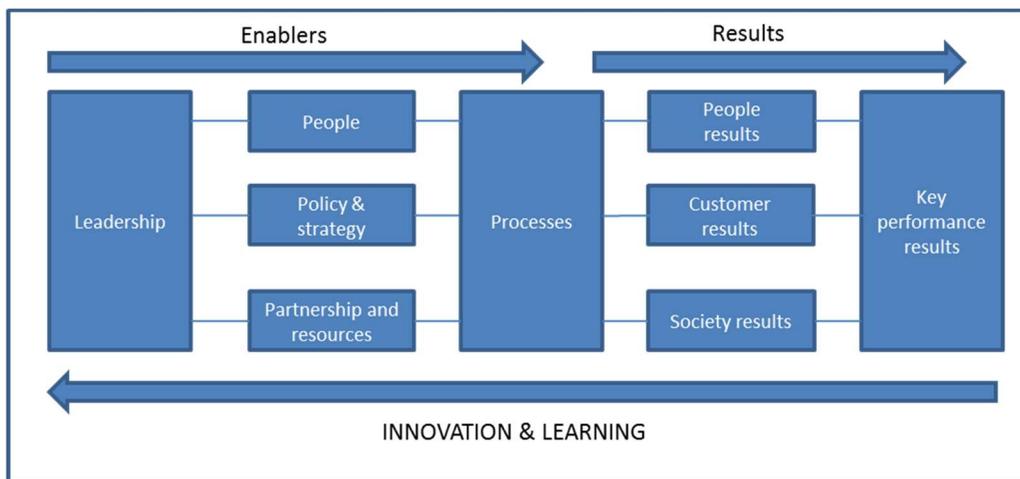


Ilustración 2. Modelo de excelencia EFQM. Fuente: Trott, 2009.

Como se puede observar en la ilustración 2, la estructura del modelo divide a la organización en nueve partes denominadas criterios (cada uno de los rectángulos). Cada criterio se refiere a los distintos aspectos o temas que el modelo plantea trabajar. A su vez cada criterio se divide en varios subcriterios, lo que permite desagregar el tema a tratar en aspectos más pequeños y concretos, lo que facilita su comprensión y aplicación. Cinco de estos criterios se denominan agentes facilitadores (*Enablers*), estos son: liderazgo, personas, política y estrategia, alianzas y recursos, y procesos. Estos criterios tratan sobre lo que la organización hace y cómo lo hace. Se trabajan cuestiones como la capacidad de los dirigentes, la identidad corporativa, la planificación estratégica, la gestión de los RRHH, la gestión de los recursos materiales, la gestión de las alianzas y colaboraciones y el sistema de gestión de la organización.

Al igual que la mayoría de los sistemas de gestión de la calidad, el sistema de gestión propuesto por el modelo EFQM de excelencia es el de gestión basado en procesos, en donde los otros cuatro criterios se denominan resultados, en concreto: clientes, personas, sociedad y claves.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

Estos criterios tratan sobre lo que la organización consigue (Araújo & Sampaio, 2014; Du, Yao, & Hu, 2012; Gómez-Gómez, Martínez-Costa, & Martínez-Lorente, 2016; Jaeger & Matyas, 2016).

En este sentido a continuación, se señalan las siguientes cualidades más destacadas del modelo según las investigaciones consultadas:

- Ser un modelo de Gestión de la Calidad Total.
- Ser muy amplio y profundo como modelo orientado hacia la excelencia que es. Amplio en el sentido de que abarca todos los aspectos, áreas y ámbitos de la organización y profundo debido a que ahonda mucho en el análisis de cada uno de ellos.
- Representar un marco de trabajo para la gestión de cualquier tipo de organización: empresas con ánimo de lucro, centros educativos, administraciones públicas, entidades sin ánimo de lucro, etc.
- Permitir evaluar el desempeño de toda la organización en el camino hacia la excelencia y posibilitar compararlo con otras organizaciones, incluso de diferentes sectores.
- Servir como herramienta para realizar una autoevaluación. Este proceso permite identificar puntos fuertes y áreas de mejora, representando el sistema de mejora continua integral que incorpora el Modelo EFQM.
- Promover intensamente la participación de todas las personas de la organización en el proceso de implantación y de mejora continua, lo que supone una buena aceptación en las organizaciones.
- Permitir una alta flexibilidad en la implantación y, por lo tanto, mejorar la autorregulación de la entidad en dicho proceso. En este sentido y dada la amplitud y profundidad del modelo, éste

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

permite progresar en los ámbitos que la entidad considere prioritarios o más estratégicos (personas, procesos, indicadores, colaboraciones, planificación, etc.).

- Ser un sistema perfectamente compatible con otras normas, modelos, herramientas o códigos éticos.

Con una visión focalizada en las agencias de I+D+i, se presenta el siguiente cuadro resumen donde se describen los criterios y subcriterios de los agentes facilitadores bajo el marco del modelo EFQM para agencias de innovación gubernamentales y regionales que apoyan las actividades de innovación dentro de las empresas y del sector académico, a través de un enfoque holístico y universal hacia la excelencia en el manejo de su estrategia (EFQM, 2012). Este resumen será contrastado con los resultados reflejados en el análisis DAFO presentado por el INCIBE (2015).

	<b>Criterio (modelo EFQM)</b>	<b>Subcriterio (modelo EFQM)</b>	<b>Diagnóstico del ecosistema de ciberseguridad de España dentro del marco I+D+i. (Análisis DAFO)</b>
<b>Facilitadores</b>	<b>Liderazgo</b>	1a. Líderes desarrollan la misión, visión, valores y ética, actuando en todo momento como modelo a seguir.	Debilidad 4A.
		1b. Líderes definen, monitorizan, revisan y conducen las mejoras de los sistemas y el desempeño de la organización.	Debilidad 4B.
		1c. Líderes comprometen a las partes interesadas.	Debilidad 4C.
		1d. Líderes refuerzan la cultura de la excelencia en las personas de la organización.	Debilidad 1B.
		1e. Líderes se aseguran que la organización es flexible y maneja efectivamente el cambio.	Amenaza 3B.
	<b>Estrategia</b>	2a. La estrategia está basada en el entendimiento de las necesidades y expectativas de las partes interesadas y el entorno de la organización.	Debilidades 1A, 1B, 4B 4D y 6C.
		2b. La estrategia está basada en el entendimiento del desempeño interno y las capacidades de la organización.	Debilidades 1A, 1B, 4B 4D y 6C.
		2c. La estrategia y las políticas de soporte son desarrolladas, revisadas y actualizadas.	Debilidades 1A, 1B, 4B 4D y 6C.
		2d. La estrategia y las políticas de soporte son comunicadas, implementadas y monitoreadas.	Debilidad 1A, 1B, 4B 4D y 6C.
	<b>Personas</b>	3a. Los planes de las personas apoyan la estrategia de la organización.	Debilidad 4B, 6A, 6B y 6C.
		3b. El conocimiento y las capacidades de las personas son desarrollados.	Debilidad 4B, 6A, 6B y 6C.
		3c. Las personas están alineadas, involucradas y empoderadas.	Debilidad 4B, 6A, 6B y 6C.
		3d. Las personas se comunican de forma efectiva a través de la organización.	Debilidad 4B, 6A, 6B y 6C.

		3e. Las personas son recompensadas, reconocidas y atendidas.	Debilidad 4B, 6A, 6B y 6C.
Facilitadores	Asociación y recursos	4a. Socios y proveedores son gestionados para un beneficio sostenible.	Debilidad 1A, 1B. 3 A 4C y 5B.
		4b. Las finanzas son gestionadas para asegurar el éxito sostenible.	Amenaza 1A y debilidad 1B.
		4c. Facilidades, equipos, materiales y recursos naturales son manejados de manera sostenible.	No considerado en análisis DAFO.
		4d. La tecnología es gestionada para soportar la estrategia.	Amenaza 3A.
		4e. La información y el conocimiento son gestionados para soportar la toma de decisión y el desarrollo de las capacidades de la organización.	Debilidad 5B y amenaza 3C.
	Procesos, productos y servicios	5a. Los procesos son diseñados y gestionados para optimizar el valor de las partes interesadas.	Debilidad 1A, 1B 4C, 5A y 6C.
		5b. Los servicios son desarrollados para la creación de optimo valor a los clientes	Debilidad 1A, 1B 4C, 5A y 6C.
		5c. Productos y servicios son efectivamente promovidos y comercializados.	Debilidad 1A, 1B 4C, 5A y 6C.
		5d. Servicios son producidos, entregados y gestionados	Debilidad 2A, 2B y amenaza 2A.
		5e. La relación con el cliente es gestionada y comprometida	Debilidad 2A, 2B y amenaza 2A.

Tabla 2. Relación de los criterios de los facilitadores del modelo EFQM con el diagnóstico de ciberseguridad en España dentro del marco I+D+i. Fuente: Elaboración propia

Al intentar diagnosticar la necesidad del modelo con la información detectada por el INCIBE, se evidencia la falta de profundidad y detalle en los 9 criterios considerados en el modelo EFQM, por lo cual solo los facilitadores pueden ser considerados en la Tabla 5 excluyéndose los criterios resultados. Siendo las cosas así, resulta clara la necesidad de realizar un cuestionario más específico a los agentes involucrados en este ecosistema que permita detectar el grado de madurez de los criterios y subcriterios de dicho modelo.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

Así mismo, al intentar diagnosticar el comportamiento del ecosistema con la información detectada queda en evidencia la práctica inexistencia de estudios y estadísticas específicas que permitan la realización de un análisis sistemático. Esto obedece en gran medida, a ser la ciberseguridad un concepto relativamente novedoso y emergente. Adicionalmente, se trata de un área transversal, con aplicaciones prácticamente en todos los ámbitos de las Tecnologías de la Información y las Comunicaciones (TIC) y en todos los sectores productivos, lo que hace complejo la obtención de datos económicos que permitan cuantificar tanto la industria como el nivel de I+D+i de ésta (Cendoya, 2016; INCIBE, 2015, 2016).

Sin embargo, esta valiosa información detectada ha permitido al INCIBE reconocer la necesidad de fundar una agencia de innovación estableciendo su misión, visión, valores, objetivos estratégicos, líneas de acción y medidas. Es por esto, que luego del contraste de aportaciones antes expuesto es posible establecer las siguientes necesidades detectadas en el ecosistema:

- Necesidad de una estructura que permita definir e implementar una estrategia en I+D+i en el ecosistema de ciberseguridad de España (justificación de instauración del RENIC).
- Necesidad de una herramienta de autoevaluación utilizada por el RENIC, que permita medir y evaluar como el ecosistema de ciberseguridad dentro del marco I+D+i funciona en la búsqueda de la excelencia en la implantación de su estrategia.

## **2.4 Red de Excelencia Nacional de Investigación en Ciberseguridad.**

Como se ha mencionado anteriormente, la necesidad de una estructura que permita definir e implementar una estrategia en I+D+i en el ecosistema de ciberseguridad de España se ha visto solventada con la instauración del RENIC, siendo conveniente considerar la definición de la estrategia que esta institución plantea. Para esto, se citan los estatutos establecidos en la página oficial (RENIC, 2016. Presentación del RENIC a la industria de ciberseguridad. Recuperado de <http://www.renic.es/es/index.html>):

- Misión: La razón de ser del RENIC es contribuir a la mejora de la competitividad investigadora en ciberseguridad, buscando el desarrollo de soluciones que mitiguen los riesgos y amenazas emergentes, dando respuesta a necesidades del mercado. Para ello, se potencia la coordinación y la cooperación activa a través de iniciativas que permitan explotar las capacidades del ecosistema investigador en ciberseguridad de forma colaborativa, sinérgica y conjunta.
- Visión: Posicionar el ecosistema de I+D+i en ciberseguridad dentro de la arena global como un ecosistema competitivo, con altos niveles de transferencia y valoración tecnológica y con un alto grado de colaboración y conexión entre sus agentes.

De igual forma, en la misma fuente, el RENIC declara que la excelencia, la practicidad, el rigor, la transparencia, la confianza, el espíritu de equipo y la dimensión internacional son los

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

valores institucionales (RENIC, 2016). Así mismo, INCIBE (2015) propuso dos premisas como bases elementales de la red:

- Participación de todos los tipos de agentes del ecosistema (Administraciones Publicas, Organismos de soporte a la I+D+i, la industria y el sector académico).
- Permitir distintos modelos de colaboración (público-privado, privado-privado, público-público).

De forma similar, en lo relativo al liderazgo y la coordinación de la red se propuso un modelo mixto transversal-nodal, en el cual se integran dos metodologías de acción dentro de la red. El enfoque transversal propone un modelo abierto para la participación de todos los agentes del ecosistema que así lo deseen buscando la integración y abarcando la ciberseguridad desde una perspectiva común y general. De igual manera, el enfoque nodal considera la participación de los agentes “mejores de su clase”, buscando así la mayor aportación posible a través de los nodos especializados en temáticas concretas. Estos nodos tendrán como filosofía la orientación a la excelencia y estarán interconectados entre ellos, componiendo una “trama de nodos” que conecte diferentes partes del ecosistema, creando así una masa crítica global de excelencia (INCIBE, 2015).

Resulta relevante señalar ante esto, que el modelo EFQM exige como requisito indispensable para su implementación la orientación hacia la excelencia en sus objetivos, por lo que la propuesta de implantación del modelo EFQM en el RENIC que se busca en esta investigación será considerada como parcial por considerar solo aquellos objetivos que estén orientados a la excelencia bajo el enfoque nodal mencionado.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

A continuación se presentan los objetivos estratégicos de esta institución bajo el enfoque nodal, siendo estos los considerados para la implantación del modelo parcial de excelencia EFQM (RENIC, 2016. Presentación del RENIC a la industria de ciberseguridad. Recuperado de <http://www.renic.es/es/index.html>):

- Fomento de la excelencia de los equipos de investigación avanzada en ciberseguridad nacional potenciando sus capacidades y aumentando el grado de colaboración y conexión entre sus agentes.
- Mejorar la conexión del sector académico-investigador con la industria de ciberseguridad potenciando la transferencia de tecnología y conocimiento.
- Fomentar la difusión y promoción de los resultados de la I+D+i de excelencia.
- Identificar, atraer, generar, retener y desarrollar profesionales en ciberseguridad a nivel nacional.
- Actuar como facilitador para encontrar fórmulas de financiación para que los agentes del ecosistema puedan financiar sus proyectos de I+D+i en ciberseguridad.

En este sentido, al ser este un modelo basado en la excelencia, su implementación se plantea como la herramienta necesaria para el buen funcionamiento e integración entre los agentes especializados del ecosistema, incidiendo de manera positiva sobre las acciones que deberán desarrollar dichos agentes para alcanzar los objetivos planteados bajo este enfoque. Así mismo, el modelo brinda una revisión periódica del desarrollo de estas actividades orientadas al logro de dichos objetivos (Du et al., 2012; EFQM, 2012; INCIBE, 2015; Gómez-Gómez et al., 2016; Jaeger & Matyas, 2016).

Ante estos planteamientos y con una visión focalizada en las agencias de I+D+i, es necesario unificar los conceptos fundamentales EFQM de la excelencia con el ecosistema de ciberseguridad dentro del marco I+D+i que el RENIC aspira liderar. Ya que, es a través de estos conceptos que se definirán los resultados que busca alcanzar la implantación del modelo parcial.

## 2.5 Conceptos fundamentales de la excelencia

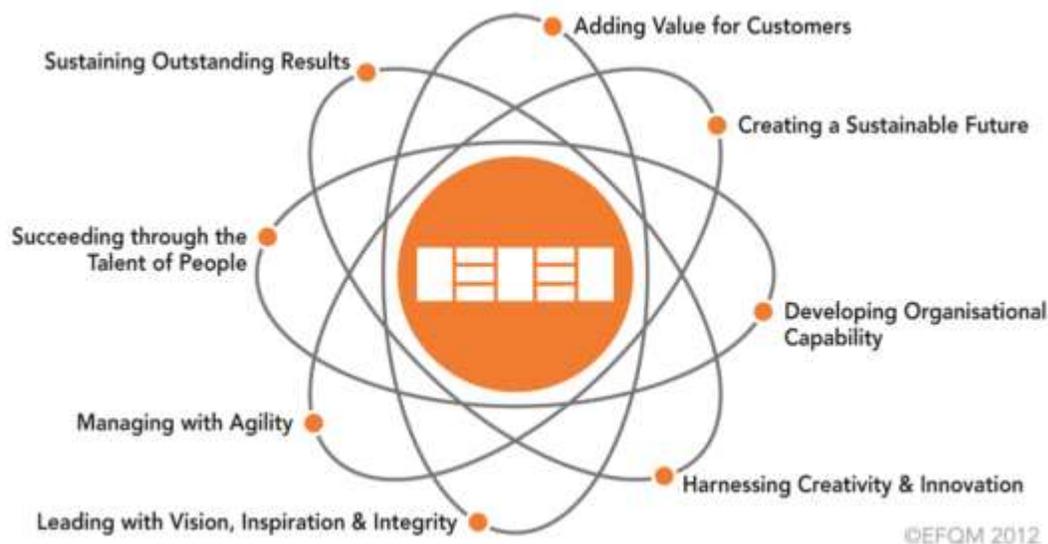


Ilustración 3. Conceptos fundamentales EFQM de la excelencia. Fuente: EFQM (2012).

EFQM (2012), en la ilustración 3 presenta los cimientos para la obtención de excelencia sostenible en cualquier tipo de organización. Estos conceptos fundamentales pueden ser utilizados como base para describir los atributos de la cultura en organizaciones orientadas a la excelencia, además de servir como herramienta de lenguaje común entre altos directivos de organizaciones. En este sentido a continuación, se describe el alcance de las acciones que se espera lleven a cabo

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

organizaciones orientadas a la excelencia bajo cada concepto fundamental que considera el modelo en estudio:

- Que adhieran valor para los clientes (*Adding value for costumers*): Las organizaciones excelentes constantemente buscaran adherir valor entendiendo, anticipando y cubriendo las necesidades, expectativas y oportunidades desde la perspectiva del consumidor.

- Que generen un futuro sostenible (*Creating a sustainable future*): Las organizaciones excelentes tendrán un impacto positivo sobre el entorno en el que se desenvuelven mejorando su rendimiento y simultáneamente impulsando el avance económico, ambiental y social dentro de las comunidades a las cuales involucra.

- Que desarrollen la capacidad organizacional (*Developing organizational capacity*): Las organizaciones excelentes mejoraran su rendimiento mediante una efectiva gestión del cambio dentro y más allá de los límites de la organización.

- Que aprovechen la creatividad y la innovación (*Harnessing creativity and innovation*): Las organizaciones excelentes generarán mayor valor y niveles de desempeño a través de mejoras continuas e innovaciones sistemáticas aprovechando la creatividad de sus agentes involucrados.

- Que lideren con visión e integridad (*Leading with vision, inspiration and integrity*): Las organizaciones excelentes poseerán líderes que den forma al futuro haciéndolo posible, actuando como modelo a seguir por sus valores y sus planteamientos éticas.

- Que gestionen con agilidad (*Managing with agility*): Las organizaciones excelentes serán ampliamente reconocidas por su habilidad de identificar y responder de manera eficiente y efectiva ante oportunidades como ante amenazas.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

- Que tengan éxito a través del talento de la gente (*Succeeding through the talent of people*):

Las organizaciones excelentes valorarán a su gente y crearán una cultura de empowerment para la obtención de objetivos tanto organizacionales como personales.

- Que mantengan resultados excepcionales (*Sustaining outstanding results*): Las organizaciones excelentes alcanzarán mantener resultados excepcionales que permitan cubrir las necesidades a corto y largo plazo de los agentes, dentro del contexto operacional en el que se desenvuelven.

De igual manera, EFQM (2012) propone un marco referencial para cada criterio del modelo estableciendo en cada uno de ellos lo esperado por las agencias de innovación orientadas a la excelencia basado en los ocho conceptos fundamentales presentes en la ilustración 3. Este marco sirve de base para contrastar cada objetivo estratégico nodal establecido por el RENIC, permitiendo definir las expectativas por cada criterio que se espera alcanzar.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

Objetivo estratégico del RENIC	Criterio (Facilitador) del modelo EFQM	Expectativas de agencias de innovación orientadas a la excelencia (Modelo EFQM)
Fomento de la excelencia de los equipos de investigación avanzada en ciberseguridad nacional potenciando sus capacidades y aumentando el grado de colaboración y conexión entre sus agentes.	Liderazgo	Establecer y comunicar una dirección clara y enfoque estratégico; Integrando a sus agente para compartir y alcanzar la Misión, la Visión y las metas de la organización.
	Estrategia	Unificar las necesidades y expectativas de las partes interesadas para contribuir al desarrollo y revisión de su estrategia y políticas de apoyo, permaneciendo alerta a cualquier cambio.
	Personas	Definir las habilidades, competencias y niveles de desempeño de las personas requeridas para alcanzar la Misión, la Visión y los objetivos estratégicos.
	Asociación y recursos	Segmentar agentes en base a la estrategia (nodal) de la organización y adoptar políticas y procesos apropiados para trabajar de manera conjunta aspirando alcanzar la visión establecida por la organización.
	Procesos, productos y servicios	Desarrollar una mezcla significativa de indicadores de desempeño de procesos y medidas de resultados relacionados, que permitan revisar la eficiencia y la efectividad de los procesos clave y sus contribuciones hacia los objetivos estratégicos.
Mejorar la conexión del sector académico-investigador con la industria de ciberseguridad potenciando la transferencia de tecnología y conocimiento.	Liderazgo	Definir y utilizar un conjunto equilibrado de resultados para revisar el progreso, ofrecer una visión de las prioridades a largo y corto plazo y gestionar las expectativas de los principales interesados
	Estrategia	Comparar su desempeño con puntos de referencia relevantes que permitan entender sus fortalezas relativas y áreas de mejora.
	Personas	Alinear los planes de personas de todos los agentes del ecosistema con la estructura operativa de la red considerando las nuevas tecnologías y los procesos clave de la organización.
	Asociación y recursos	Asegurar que sus líderes reciban información precisa y suficiente para apoyarlos en la toma de decisiones oportunas
	Procesos, productos y servicios	Esforzarse por innovar y crear valor para sus clientes, involucrándolos y otras partes interesadas, y cuando proceda, en el desarrollo de productos, servicios y experiencias nuevos e innovadores.

**Tabla 3. Expectativa de criterio facilitador por objetivo estratégico del RENIC. Fuente: Elaboración propia.**

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

Objetivo estratégico del RENIC	Criterio (Facilitador) del modelo EFQM	Expectativas de agencias de innovación orientadas a la excelencia (Modelo EFQM)
Fomentar la difusión y promoción de los resultados de la I+D+i de excelencia.	Estrategia	Crear, difundir, promover y mantener una estrategia clara y políticas de apoyo para lograr la Misión y la Visión de la organización
	Personas	Crear una cultura de creatividad e innovación en toda la organización, asegurando que las personas tengan una mentalidad abierta y puedan responder rápidamente a los desafíos que enfrentan
	Asociación recursos	y Diseñar el proceso de planificación financiera, control, presentación de informes y revisión para apoyar el uso óptimo de los fondos públicos, al tiempo que se asegura la rendición de cuentas y la transparencia de la organización.
	Procesos, productos servicios	y Supervisar y revisar continuamente las experiencias y percepciones de sus clientes y asegurar que los procesos estén alineados para responder apropiadamente a cualquier feedback.
Identificar, atraer, generar, retener y desarrollar profesionales en ciberseguridad a nivel nacional.	Liderazgo	Comprender y desarrollar las capacidades subyacentes de la organización, / Inspirar a las personas y crear una cultura de participación, apropiación, empoderamiento, mejora y rendición de cuentas a través de sus acciones, comportamientos y experiencia.
	Estrategia	Identificar y comprender los resultados clave requeridos para lograr su Misión y evaluar el progreso hacia la Visión y los objetivos estratégicos.
	Personas	Motivar a las personas a involucrarse en la mejora y la innovación y reconocer sus esfuerzos y logros.
	Asociación recursos	y Comunicar una dirección clara y un enfoque estratégico para asegurar que las personas entiendan y puedan demostrar su contribución al éxito continuo de la organización.
Actuar como facilitador para encontrar fórmulas de financiación para que los agentes del ecosistema puedan financiar sus proyectos de I+D+i en ciberseguridad.	Liderazgo	Involucrar y buscar el apoyo y las contribuciones de todas las partes interesadas relevantes para los cambios necesarios para asegurar el éxito sostenible de la organización.
	Estrategia	Traducir sus estrategias en procesos alineados, proyectos y estructuras organizativas sostenibles.
	Personas	Promover una cultura de apoyo mutuo, reconocimiento y cuidado entre individuos y entre equipos.
	Asociación recursos	y Utilizar estrategias, políticas y procesos para administrar edificios, equipos y materiales de manera sostenible desde el punto de vista financiero y ambiental
Procesos, productos servicios	Comparar el desempeño de la red con puntos de referencia relevantes que permitan detectar las y fortalezas y oportunidades de mejora para maximizar el valor generado por los clientes.	

**Tabla 4. Expectativa de criterio facilitador por objetivo estratégico del RENIC (Cont.). Fuente: Elaboración propia.**

Este contraste deja en evidencia cómo los objetivos estratégicos del RENIC bajo el enfoque nodal están coherentemente orientados a la búsqueda de la excelencia (INCIBE, 2015) y las expectativas de agencias innovadoras bajo el modelo EFQM están alineadas con lo que se espera alcanzar de estos objetivos planteados (EFQM, 2012). Permitiendo así, establecer un punto de convergencia entre ambas fuentes que sirve de base para considerar el nivel esperado en los criterios facilitadores del RENIC como agente propulsor del I+D+i en la ciberseguridad de España.

Así mismo, alcanzar resultados balanceados es uno de los conceptos fundamentales detrás del Modelo de Excelencia EFQM por lo que es necesario para las agencias de innovación públicas, que normalmente cuentan con un conjunto complejo de actores que a su vez plantean diferentes expectativas sobre las actividades de la organización, el uso de una herramienta que les permita medir como la organización se está desempeñando y que a su vez, ayude a entender y superar las necesidades existentes que la alejan de alcanzar la excelencia en la implantación de su estrategia.

## **2.6 Proceso de autoevaluación en modelo de excelencia EFQM**

Para esto, el modelo EFQM incluye el *Self-assessment process* (Proceso de autoevaluación), que juega un rol trascendental para la obtención de mejoras en las organizaciones, ya que la lleva a lograr la implementación de sus estrategias obteniendo los resultados esperados a través de una visión holística del estado de la organización. Esto obedece a que este proceso le permite a la organización discernir claramente sus puntos fuertes y las áreas de mejora, y culmina en acciones planificadas que luego son monitoreadas para el progreso. En la Ilustración 4 se muestra la secuencia de etapas que lleva el desarrollo del proceso de autoevaluación.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto



Ilustración 4. *Self-Assessment* en Modelo de excelencia EFQM. Fuente Elaboración Propia.

Como se evidencia en la ilustración 4, es necesario que los participantes posean conocimientos suficientes sobre los objetivos estratégicos de la organización y conocimientos suficientes del modelo, ya que se requiere una visión general de la organización para participar en esta autoevaluación. Por consiguiente, esta actividad que además de contar con fuentes de información de todos los agentes de la organización, es realizada por cargos directivos y gerenciales, ya que a través de este proceso se busca definir las líneas de acciones a seguir para lograr los objetivos estratégicos.

Este proceso considerado en el modelo EFQM será posible en las agencias de innovación siempre que se desarrollen las seis etapas que contempla el *Self-assessment process*, en la que se deberá implementar una estructura que permita medir la satisfacción y expectativas de los agentes. Esto se logra agrupando las mediciones en cuatro categorías: clientes, personas, sociedad y resultados claves. Al igual que en todas las mediciones, el enfoque debe ser orientado hacia las tendencias y comparaciones y no sólo hacia los resultados mismos. Ante esto, EFQM (2012)

plantea las siguientes medidas e indicadores para agencias de innovación, las cuales serán consideradas para la propuesta del modelo parcial de excelencia EFQM para la ciberseguridad en España.

Criterio	Sub criterio	Medidas a incluir en agencias de innovación
Resultados de los clientes	Percepción	Valor adherido percibido de diferentes productos y servicios
		Servicio y soporte al consumidor para los diferentes segmentos
		Imagen y reputación en comparación con puntos de referencia relevantes
	Desempeño	Tiempo de rendimiento del producto / servicio ofrecido
		Numero de quejas
		Nivel de interacción con clientes
Resultados de las personas	Percepción	Satisfacción, participación y compromiso
		Orgullo y cumplimiento
		Liderazgo y gestión
		Definición de objetivos, gestión de la competencia y el desempeño
		Competencia, entrenamiento y desarrollo de carrera
		Comunicación efectiva
		Condiciones de trabajo
	Desempeño	Participación y compromiso
		Definición de objetivos, gestión de la competencia y el desempeño
		Desempeño de liderazgo
		Entrenamiento y desarrollo de carrera
Resultados de la sociedad	Percepción	Reputación e imagen a través de encuestas
		Impacto ecológico de los procesos internos de la agencia
		Avances en asuntos sociales asociados al entorno
		Reconocimiento y reputación en medios
	Desempeño	Impacto ecológico de los procesos internos de la agencia
		Actividades internas enmarcadas en el bienestar social y ambiental
Resultados claves	Percepción	Éxito ante los indicadores de desempeño acordados con el ente supervisor
		Resultados de proyectos financiados / liderados
		Desarrollo de compañías clientes (agentes)
		Indicadores de innovación (numero de patentes en proyectos)
	Desempeño	Costos de operación
		Alineación de los proyectos y el portafolio de productos/servicios de las compañías clientes (agentes) con los objetivos estratégicos
		Uso controlado de los recursos
		Resultados obtenidos como intermediario para la obtención de financiaciones

Tabla 5. Percepción y desempeño en agencias de innovación bajo el modelo EFQM. Fuente: (EFQM, 2012)

## **2.7 Quick Self-Assessment del modelo de excelencia EFQM**

Con una visión focalizada en la investigación, EFQM (2012) propone un *quick self-assessment* para organizaciones de innovación que deriva de las etapas “Conducir la Evaluación” y “Acordar prioridades” del proceso de autoevaluación antes descrito. Este instrumento, a pesar de no poder ser considerado como un proceso de autoevaluación, puede ser utilizado como un primer paso para las agencias de innovación en su camino a la excelencia, ya que con 20 preguntas de autoevaluación sobre la organización que permiten visualizar su madurez desde cada concepto fundamental de la excelencia, además facilita la unificación de criterios entre los agentes sobre el impacto de las acciones a seguir para lograr alcanzar de manera eficaz y eficiente la excelencia que se aspira. En la ilustración 5 se resume el alcance de este instrumento de diagnóstico.

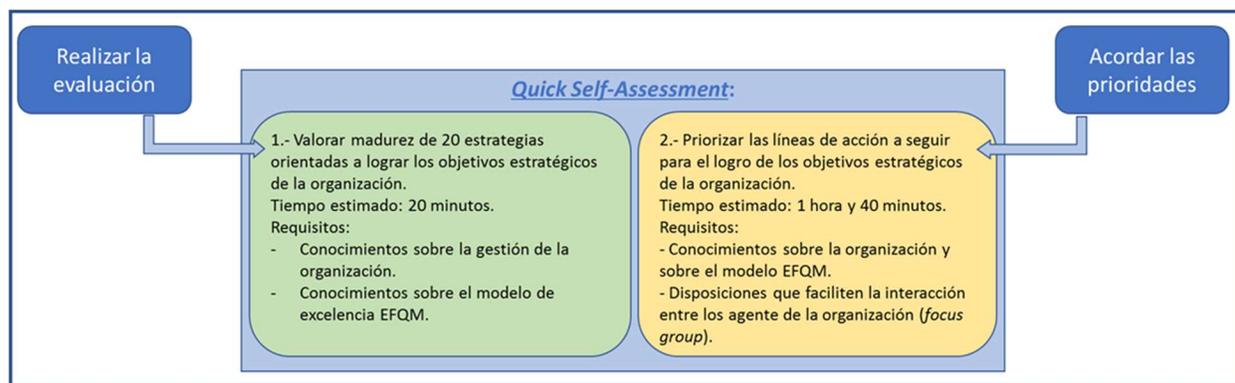


Ilustración 5. Estructura del *Quick Self-Assessment*. Fuente: Elaboración propia.

Este instrumento, incluido en el anexo II, permite conocer si existe la necesidad de implementar un modelo de excelencia EFQM en agencias de innovación a través del diagnóstico de la gestión central de la organización, buscando detectar claras oportunidades de mejora basado

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

en la madurez y el impacto de la estrategia de la organización. Además, permite evaluar la consistencia de la estructura implantada en el desarrollo de las estrategias, logrando a través de su aplicación, detectar si la organización evaluada cuenta con las facultades para implementar el modelo (EFQM,2012). En este sentido, se presenta como una herramienta de autoevaluación del desempeño de los agentes y de ayuda en la detección de las oportunidades de mejora orientadas a la excelencia de los resultados del ecosistema.

En este sentido, EFQM (2012) propone un *quick self-assesment* (Autoevaluación rápida) para agencias de innovación que ofrece una visión global de las capacidades de la organización, siendo a su vez contrastadas con los conceptos fundamentales EFQM de la excelencia. Sin embargo, al igual que con el *Self,-Assesment Process* (Proceso de autoevaluación), resulta de suma importancia que los agentes involucrados posean suficientes conocimientos sobre la organización a la que pertenecen y sobre el funcionamiento del modelo EFQM.

Ante esto, se pueden resumir atendiendo a las fuentes consultadas hallazgos relevantes como lo es el escaso desarrollo de investigaciones académica sobre la gobernanza en ciberseguridad dentro del marco I+D+i. Además, se detectó la inexistencia de un plan específico de ciberseguridad dentro del marco I+D+i en España (INCIBE, 2015). De igual manera, ha quedado clara la necesidad de establecer indicadores que permitan medir el desempeño de los agentes del ecosistema para conseguir los objetivos que el RENIC se plantea orientados a la excelencia.

Para esto, el modelo de EFQM se presenta como un buen punto de partida con vistas a establecer el plan de acciones a emprender para lograr la excelencia. Además, por su orientación

y su continua mejora, encaja perfectamente con el dinamismo que la ciberseguridad requiere en su constante búsqueda de soluciones que mitiguen las cambiantes y crecientes amenazas que representan el uso del ciberespacio. Adicionalmente, el *quick self-assessment* se presenta como como el mecanismo ideal para realizar un primer diagnóstico sobre el funcionamiento actual del ecosistema, además permite evaluar la necesidad de la implementación de un modelo EFQM. Por lo cual, parece oportuno consultar a los agentes relevantes del ecosistema si las estrategias propuestas actualmente por el RENIC poseen la madurez necesaria para alcanzar los objetivos establecidos.

### **3 MARCO METODOLÓGICO**

---

En este capítulo se explica el fundamento metodológico en el que se sustenta el desarrollo de esta investigación. Para esto, según Hernández, Fernández y Baptista (2006) se puede establecer que esta investigación de tipo descriptiva presenta un enfoque mixto, donde lo cuantitativo es definido como aquel enfoque que usa la recolección de datos para probar una hipótesis, con base en la medición numérica y el análisis estadístico para establecer patrones de comportamiento y probar teorías. En este sentido, esta investigación se encasilla bajo este enfoque por cumplir los requerimientos que se explicitan en la siguiente secuencia de etapas:

1. Plantea un problema de estudio delimitado y concreto.
2. Revisa antecedentes asociados y relevantes al problema.
3. Construye el marco teórico basado en revisiones literarias.
4. Elabora una hipótesis para su posterior prueba mediante el empleo de diseños apropiados.
5. Recolecta datos de los participantes que estudia y analiza.

De igual forma, considera el enfoque cualitativo al desarrollar acciones de recolección de datos sobre diversos conceptos (variables), aspectos, dimensiones o componentes del fenómeno a investigar (Hernández, Fernández y Baptista, 2006), quedando esto en evidencia con las acciones realizadas para la recolección de datos. Bajo estos parámetros, se derivan otras características del enfoque que se detallan en los párrafos siguientes:

### 3.1 Tipo de investigación

Según lo planteado por Hernández, Fernández y Baptista (2006) se ha desarrollado la ilustración 6 en la cual se identifican los tipos de investigación, así como los criterios en los cuales se sustenta el investigador al decidir el tipo de investigación.

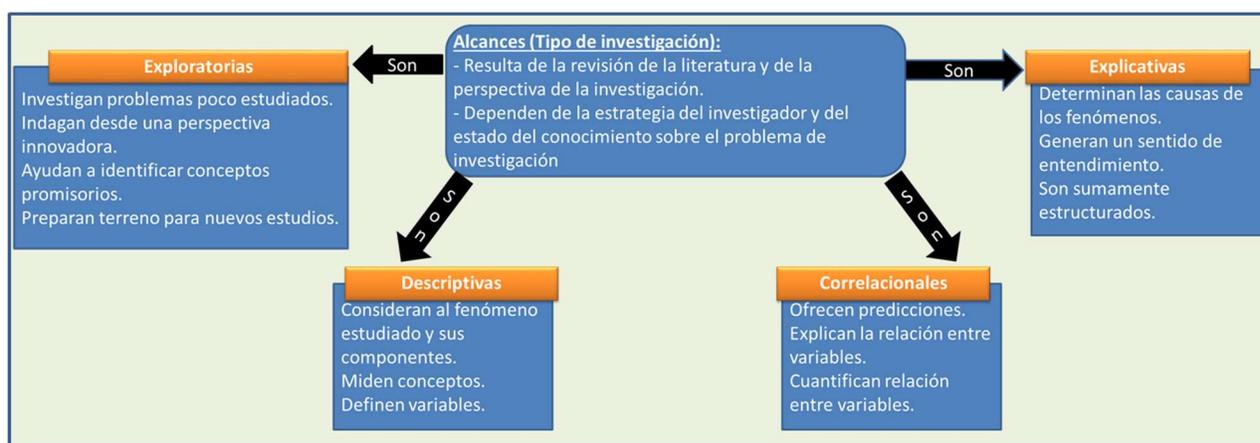


Ilustración 6. Alcances (Tipo de investigación). Fuente: Elaboración propia.

Ante esto, se puede establecer que esta investigación está enmarcada como descriptiva, ya que en ella se busca de manera sistemática recabar información relevante sobre las prácticas de gestión y gobernanza en ciberseguridad actuales en España, con especial atención en las acciones relacionadas con la gestión de la innovación y del conocimiento para ser contrastadas con las teorías de Trott (2009), Tidd (2005), Dalkir (2005) y Lugen (2004) las cuales delimitan el ámbito del estudio. Permitiendo así establecer el contexto actual de la ciberseguridad española dentro del marco I+D+i. Además, a través del modelo de excelencia EFQM y basado en su *quick self-assessment*, se plantea un instrumento de recolección de datos el cual servirá para evaluar la

madurez de las estrategias orientadas a la excelencia que el RENIC plantea para lograr sus objetivos.

### **3.2 Diseño de la investigación**

En este mismo orden de ideas, según lo expuesto por Hernández, Fernández y Baptista (2006), esta investigación se desarrolló bajo un diseño no experimental por no existir la manipulación deliberada de variables y basarse en una investigación donde se observan fenómenos tal y como se dan en su contexto natural, para luego ser analizados. De igual manera, se estructura su desarrollo bajo un diseño correlacional – causal *ib.*, por buscar describir la relación entre dos variables (Ciberseguridad de España dentro del marco I+D+i y Excelencia) en un momento determinado (momento actual) y estableciendo una relación causal entre ambas a través de la propuesta del modelo parcial de excelencia EFQM.

### **3.3 Población y muestra**

Para este estudio, se considera como población el ecosistema I+D+i delimitado por el INCIBE (2015), el cual se divide en 4 grandes bloques: administraciones publicas, organismos de soporte I+D+i, sector académico e industria. De los cuales serán utilizados como muestra 33 participantes de los agentes relevantes del sector académico que participaron en el estudio de viabilidad y diseño del RENIC, a los cuales se les hizo llegar el cuestionario desarrollado para determinar la necesidad de un modelo de excelencia EFQM, además de la percepción del

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

encuestado sobre las capacidades tanto del RENIC como del ecosistema para llevar a cabo dicha implementación.

De igual manera, para la realización de la entrevista al experto se considera al director de I+D+i de una empresa privada perteneciente al sector industrial que participo en el estudio antes citado realizado por el INCIBE (2015). Esta empresa cuenta con una amplia trayectoria internacional en proyectos de gran envergadura de I+D+i y posee certificaciones vigentes en gestión de la calidad (ISO 9001), en gestión I+D+i (UNE 166002) y en gestión de la seguridad de la información (ISO 27001). Esta entrevista semiestructurada basada en el protocolo considerado en el Anexo VI busca determinar la necesidad de un modelo de excelencia EFQM, además de la percepción del encuestado sobre las capacidades tanto del RENIC como del ecosistema para llevar a cabo dicha implementación.

### **3.4 Técnica e instrumento de recolección de datos**

Para esta investigación, se desarrollaron dos técnicas para la recolección de datos basados en la etapa en la que se define el grado de madurez de las estrategias (Realizar la evaluación) del *quick self-assessment*. En ambas técnicas se busca establecer desde la perspectiva de los consultados la necesidad de un modelo de excelencia EFQM, además de su percepción sobre las capacidades tanto del RENIC como del ecosistema para llevar a cabo la implementación de dicho modelo.

**Cuestionario orientado a determinar la necesidad de un modelo parcial de excelencia EFQM para desarrollo del ecosistema de ciberseguridad en España dentro del marco I+D+i.**

Cumpliendo con la metodología de aplicación propuesta por el autor, se selecciona para la realización de esta actividad solamente a agentes del sector académico por las siguientes razones:

1.- La teoría establece que el encuestado deberá poseer suficientes conocimientos sobre la organización, su misión, visión y objetivos, ante lo cual el sector académico lleva una ventaja con respecto a los otros 3 bloques presentes en el ecosistema por estar la junta directiva del RENIC conformada en su totalidad por representantes pertenecientes a este sector.

2.- El conocimiento del modelo EFQM exigido para la realización del cuestionario solo podría ser confirmado en los encuestados si se desarrolla la etapa de entrenamiento a los participantes (Capacitar a los participantes). Esta limitante está presente en los 4 bloques de la población. Sin embargo, por estar asociadas la estructura del instrumento a los objetivos estratégicos del RENIC, es posible que esta limitación sea superada por agentes del sector que posean suficientes conocimientos de la organización.

3.- Debido a los controles de información y medidas de seguridad asumidas por muchos de los agentes considerados en la población, el relativamente fácil acceso a los correos electrónicos del sector académico a través del internet realza a este bloque por encima del resto.

El cuestionario fue difundido el 28/02/2017 a través de un correo electrónico en el cual fueron descritas las motivaciones y objetivos. Además, se incluyó el enlace:

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

[https://docs.google.com/forms/d/e/1FAIpQLSc9m4Ch7GQPxBWHX19s8\\_uEyLF0fff8EKm69hHUt3-\\_pzo8lQ/viewform](https://docs.google.com/forms/d/e/1FAIpQLSc9m4Ch7GQPxBWHX19s8_uEyLF0fff8EKm69hHUt3-_pzo8lQ/viewform) en el que se daba acceso a la encuesta.

Como se comentó previamente, dicha comunicación fue difundida a 33 agentes del sector académico considerados por el INCIBE como agentes representativos del ecosistema y entre las indicaciones descritas en la comunicación, se estableció desde el 01/03/2017 hasta el 14/03/2017 como el período para completar la actividad y con un tiempo estimado para realizar el cuestionario de 10 minutos. Se consiguió como resultando la participación de 3 agentes en la investigación. Simultáneamente, se le notificó al RENIC el objeto del estudio y la necesidad de aplicar el cuestionario, ante lo cual se dio por enterado e instó a ser informado de los resultados que se obtengan como resultado de esta investigación.

A pesar de la poca participación conseguida durante la recolección de datos, no se consideró oportuno tomar medidas para aumentar esa tasa de respuesta debido a que el cuestionario aplicado busca determinar la necesidad de un modelo de excelencia, además de un diagnóstico sobre las capacidades tanto del RENIC como del ecosistema para llevar a cabo dicha implementación y ante la homogeneidad de las respuestas y la poca trayectoria del RENIC admitida por su propio presidente se considera irrelevante repetir la toma de datos. Así mismo, se debe aclarar que para obtener un diagnóstico más preciso de la necesidad de un sistema de gestión de la calidad total del RENIC, será necesario considerar a todos los sectores del ecosistema.

El instrumento aplicado consta de 20 premisas en las que se enuncian las guías de acciones a llevar a cabo por el RENIC para lograr la excelencia en sus objetivos estratégicos definidos bajo el modelo constructo-nodal. De igual manera, estas premisas están basadas en los conceptos

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

básicos de excelencia considerados en el modelo EFQM (Ver ilustración 3). Estas líneas de acción son presentadas con la opción a preguntas cerradas con opción múltiple, donde se incluyen 5 alternativas que permiten indicar el grado de desarrollo de cada línea de acción en la actualidad. Las opciones basadas en la escala Lickert, van de "Nada desarrollada" hasta "Madura con mejoras continuas".

Tabla de valores de alternativas:

- Nada desarrollada = 1
- En sus primeros pasos de desarrollo = 2
- Madura sin mejoras previstas =3
- Madura con mejoras por realizar = 4
- Madura con mejoras continuas = 5

### **Entrevista a experto**

Esta entrevista se llevó a cabo con la participación del director de I+D+i de una organización del sector privado que por su trayectoria y trascendencia tanto en ciberseguridad nacional e internacional como en I+D+i, es considerada un agente relevante por el INCIBE (2015). Esta entrevista realizada el 22/03/2017 tuvo una duración de 30 minutos y fue realizada siguiendo el protocolo incluido en el anexo VI. El protocolo de entrevista utilizado fue desarrollado, al igual que el cuestionario, para determinar la necesidad de un modelo de excelencia y para diagnosticar las capacidades tanto del RENIC como del ecosistema, para llevar a cabo dicha implementación. Se dividió en 5 etapas en las cuales se incluyeron preguntas relacionadas con el RENIC, el

ecosistema de ciberseguridad en España dentro del marco I+D+i, modelo de excelencia EFQM y el contexto nacional e internacional de actividades I+D+i en ciberseguridad. Igualmente fue considerado el *quick self-assessment* para el desarrollo de esta técnica de recolección de datos.

### **3.5 Validez y confiabilidad del instrumento**

Las técnicas utilizadas para la recolección de datos están basadas en el *quick self-assessment* para agencias de innovación propuesto por el EFQM (2012), siendo una herramienta de gran utilidad para la detección de la necesidad de implementación del modelo EFQM además de servir para diagnosticar tanto al ecosistema como al RENIC sobre sus capacidades para lograr implementar de manera exitosa dicho modelo. En este sentido, se considera que la validez y la confiabilidad del instrumento aplicado en esta investigación se sustentan en una técnica previamente validada y reconocida por el EFQM, siendo incluso recomendada como el primer paso a seguir en la iniciación para agencias de innovación que buscan diagnosticar su sistema de gestión de calidad total. Además, a través de su orientación a la excelencia disgregada en sus conceptos fundamentales, permite detectar de manera más precisa las carencias presentes en el funcionamiento de la organización.

## **4 RESULTADOS DE LA INVESTIGACIÓN**

---

Para la obtención de los objetivos propuestos se interpretó la información obtenida de cada una de las técnicas de recolección de datos aplicadas. Cumpliendo así, con lo previsto en el marco metodológico y considerando los resultados reflejados en los cuestionarios cumplimentados por los agentes representativos del sector académico del ecosistema. Además de los datos generados en la entrevista realizada al experto del sector industria.

Es importante señalar que el RENIC informó vía email electrónico (Ver anexo VII) que no contaba con registro como asociación hasta febrero del presente año, por lo cual deberá ser considerada como una entidad aún en proceso de desarrollo durante el análisis de los resultados. Esta salvedad toma gran validez al momento de entender el escaso desarrollo del RENIC en lo relativo a sus estrategias, afectando también en el alcance de sus acciones hasta la fecha y el desarrollo de su liderazgo entre sus agentes.

### **4.1 Cuestionario orientado a determinar la necesidad de un modelo parcial de excelencia EFQM para desarrollo del ecosistema de ciberseguridad en España dentro del marco I+D+i.**

#### **Análisis de resultados**

Para el análisis del cuestionario, serán consideradas las respuestas obtenidas por cada participante en cada una de las premisas propuestas manteniendo la valoración previamente establecida y respetando la siguiente fórmula:

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

$$RP = \sum (Rp1 + Rp2 \dots Rpn) / 5$$

Donde:

RP (Respuesta promedio): representa el promedio de las respuestas obtenidas de los agentes consultados en relación a la premisa propuesta.

Rpn (Respuesta de participante): se refiere a la respuesta manifestada por cada agente sobre la premisa evaluada.

En la tabla 16 se resumen las respuestas obtenidas por cada premisa considerada en el cuestionario:

No. Premisa	Concepto fundamental de excelencia	Enfoque hacia la excelencia considerado	Respuesta (promedio)	No. Premisa	Concepto fundamental de excelencia	Enfoque hacia la excelencia considerado	Respuesta (promedio)
1	<i>Mantener resultados excepcionales</i>	Proceso de planificación empresarial	Nada desarrollada	10	<i>Gerenciar con agilidad</i>	Marco del proceso definido y mapeado	Nada desarrollada
2		Proceso de establecimiento de objetivos	Nada desarrollada	11		Propiedad de proceso definida	Nada desarrollada
3		Balanced scorecard o informe de gestión de nivel superior	Nada desarrollada	12		Metodología de mejora de procesos	Nada desarrollada
4	<i>Adherir valor a los clientes.</i>	Gestión de relaciones con clientes	Nada desarrollada	13	<i>Liderar con visión, inspiración e integridad</i>	Declaraciones claras de visión, misión y valores	Nada desarrollada
5		Proceso de gestión de quejas	Nada desarrollada	14		Informe del KPI y reunión de revisión	Nada desarrollada
6		Encuesta al consumidor	Nada desarrollada	15	<i>Tener éxito a través del talento de la gente</i>	Proceso de evaluación de empleados	Nada desarrollada
7	<i>Desarrollar la capacidad organizacional</i>	Estrategia de benchmarking	Nada desarrollada	16		Encuesta a los empleados	Nada desarrollada
8		Política y directrices de la asociación	Nada desarrollada	17	<i>Aprovechar la creatividad y la innovación</i>	Investigación y análisis de mercado	Nada desarrollada
9		Crear y beneficiarse de una red	En sus primeros pasos de desarrollo	18		Estrategia de gestión del conocimiento	Nada desarrollada
				19	<i>Crear un futuro sostenible</i>	Política de gestión medioambiental	Nada desarrollada
				20		Política de CRS	Nada desarrollada

**Tabla 6. Respuestas de aplicación de cuestionario. Fuente: Elaboración propia.**

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en  
España dentro de un marco I+D+i*

Victor E. Vera Pinto

En el anexo V se incluye el detalle de las respuestas obtenidas de la aplicación del cuestionario.

### **Discusión de los resultados**

Como se evidencia, el resumen expuesto en la tabla 16 de las respuestas obtenidas de los agentes consultados del sector académico corrobora la ausencia de una política de calidad difundida en el ecosistema por parte del RENIC, reafirmando estas respuestas la ausencia de un sistema de gestión de calidad total y mucho menos un modelo de excelencia EFQM. De igual manera, estos resultados reflejan carencias en: su proceso de gestión, de planificación, de medición de resultados, de revisión de estrategias, de mejora continua entre otros. Sin embargo, es oportuno resaltar que con la aplicación del cuestionario se busca detectar, desde la perspectiva de los consultados, la necesidad de un modelo de excelencia EFQM, además de su percepción sobre las capacidades tanto del RENIC para liderar este modelo como del ecosistema para llevar a cabo dicha implementación.

Ante esto, se puede establecer que la necesidad de implementar un modelo de excelencia EFQM se hace presente entre los encuestados al manifestar la inmadurez en las estrategias descritas en las 20 premisas propuestas incluidas en el cuestionario. Estas estrategias, contemplan posturas orientadas a la excelencia a través del concepto fundamental sobre el cual son establecidas, por lo que estos resultados son traducidos a que no existe desarrollo por parte del RENIC en la búsqueda de la excelencia. Siendo esta ausencia total de orientación hacia la

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

excelencia para el logro de sus objetivos, la principal evidencia presente en los resultados sobre la necesidad de implementación del modelo.

Así mismo, en lo relativo a las capacidades del RENIC para desempeñar el rol de líder en el ecosistema, se debe señalar que EFQM (2012) establece que solo se le podrá aplicar el *quick self-assessment* a aquellas agencias de innovación que cumplan con el requisito de contemplar en su misión y sus objetivos la búsqueda de la excelencia, quedando así constatado con la aplicación del cuestionario que para los agentes consultados, el RENIC si dispone de las capacidades para implementar un modelo de excelencia EFQM. Igualmente, queda en evidencia que sus objetivos estratégicos concebidos bajo el constructo nodal (ver apartado 2.4) pueden ser desarrollados, medidos y mejorados a través de los conceptos fundamentales de la excelencia considerados en el modelo EFQM.

Finalmente, las facultades para la implantación del modelo de excelencia EFQM pudieron evidenciarse previa a la aplicación del instrumento, tanto en el modelado de la red descrito por INCIBE (2015) como por la posibilidad de integración de las premisas descritas en el *quick self-assessment con* las necesidades y expectativas de todos los agentes involucrados en la red (Tablas 7 y 8). Siendo esta condición, otro requisito exigido en las agencias de innovación para iniciar su proceso hacia la excelencia (EFQM, 2012).

Es importante señalar que por la poca participación de agentes del sector académico obtenida de la aplicación del cuestionario, se hace imposible analizar las opiniones que se desvían de la media obtenida de cada premisa. Esta limitación, como se ha aclarado con anterioridad, no desvirtúa la obtención de la información que se ha buscado alcanzar, pero invita a plantearse para

futuras investigaciones el hacer otro instrumento donde se logre una participación representativa que permita dar los primeros pasos en el diagnóstico de la RED.

## **4.2 Entrevista a experto**

El experto considerado para la realización de la entrevista fue el Director de I+D+i de una organización privada que cuenta con gran reconocimiento nacional e internacional en actividades tanto en ciberseguridad como en I+D+i. Entre sus más notables logros está el desarrollo de la primera solución española con capacidad de respuesta ante amenazas avanzadas persistentes (*advance persistant threat*) en asociación con el CCN (Centro Criptológico Nacional) y la participación como miembro fundador de ECSO (*European Cyber Security Organization*), asociación con la cual la Comisión Europea firmó en julio 2015 un acuerdo de cooperación público privada (cPPP), en el cual se espera que la Unión Europea invierta 450 millones de Euros bajo el programa de investigaciones e innovaciones propuesto en *Horizon 2020*.

Para el análisis de los resultados obtenidos de este método e recolección de datos se realizará un rastreo de la entrevista en profundidad que, estará orientado a detectar la necesidad de un modelo de excelencia EFQM y la percepción sobre las capacidades del RENIC para liderar la implantación del modelo. Por consiguiente, las categorías presentes en el rastreo realizado reflejarán la información que se busca obtener del entrevistado y las subcategorías dejarán en evidencia la percepción del agente sobre este asunto. Es necesario señalar que este método de recolección de datos se soporta en la fluidez de la interacción entre entrevistador - entrevistado, la cual permite indagar sobre los conocimientos del entrevistado sobre el área de estudio en la cual

se desarrolla la investigación, siendo esto de gran importancia para lograr dar respuesta a las inquietudes que se busca resolver.

De igual manera, de acuerdo con EFQM (2012), el entrevistado deberá poseer suficientes conocimientos sobre la organización, su misión, visión y objetivos y conocimientos del modelo de excelencia EFQM para la realización de la entrevista. Sin embargo, al igual que en el cuestionario, las carencias sobre estas áreas de conocimiento serán complementadas con la experiencia y trayectoria en procesos I+D+i en ciberseguridad. Además, la fluidez de esta técnica de recolección de datos permite al entrevistador, a través de la aplicación del protocolo (ver anexo VI), guiar el desarrollo de la actividad orientándola a debatir sobre la opinión del entrevistado.

### **Análisis de resultados**

A continuación, se presenta la transcripción y el proceso de la entrevista realizada al experto:

<b>No. preguntas:</b>	<b>1. Establecer conocimientos comunes:</b>	<b>Categoría:</b>	<b>Sub - Categoría:</b>
1A.	P: ¿Conoce usted al RENIC? R: <b>No</b> , a la fecha no lo conozco.	Capacidades del RENIC.	El entrevistado desconoce el desarrollo actual de la Red de excelencia y del RENIC.
1B	P: Como director de I+D+i de una organización privada de ciberseguridad en España y siendo considerado por el INCIBE como un agente representativo dentro del ecosistema I+D+i, ¿Tiene usted algo tipo de contacto con el RENIC? R: <b>No</b> , imagino que las comunicaciones entre el RENIC	Capacidades del RENIC.	El entrevistado a pesar de su posición estratégica en la

	y la organización a la que pertenezco se harán a través de nuestro socio director. Sin embargo, <b><u>no estoy informado de algún contacto entre el RENIC y la organización a la que pertenezco.</u></b>		organización a la que representa en procesos de I+D+i, no cuenta con ningún tipo de comunicación o contacto con el RENIC.
1C	P: ¿Conoce usted como está estructurada la RED? R: <b>No</b> , lo único que se de esa Red es que se iba a construir.	Facultades del ecosistema.	El entrevistado desconoce la estructura actual del ecosistema de ciberseguridad en España
<b>No. preguntas:</b>	<b>2. Capacidades y conocimientos del entrevistado en el área de estudio:</b>	<b>Categoría:</b>	<b>Sub - Categoría:</b>
2A	P: ¿Conoce usted el modelo de gestión de la calidad orientado a la excelencia propuesto por el <i>European Foundation Quality Management</i> (EFQM)? R: <b>No</b> .	Conocimientos del entrevistado sobre el área de estudio	El entrevistado desconoce el modelo de excelencia EFQM.
2B	P: ¿Hay algún sistema de gestión de la calidad total que usted conozca que podría ser apropiado para una red de organizaciones de ciberseguridad en el marco I+D+i? R: Para una Red en concreto no. Nosotros como organización <b><u>estamos certificados por AENOR bajo la norma UNE 16602</u></b> , lo que implica que todos los procesos I+D+i están alineados con un Sistema de gestión.	Conocimientos del entrevistado sobre el área de estudio.	El entrevistado desconoce algún sistema de gestión de calidad total.
2C	P: Entiendo por lo que me dice que la empresa a la que usted	Facultades del ecosistema.	El entrevistado como agente del ecosistema, deja en

	<p>representa cuenta con actividades de I+D+i tanto a nivel nacional como internacional, ¿Es cierto esto? R: <u>Sí.</u></p>		<p>evidencia sus capacidades para participar en procesos I+D+i.</p>
2D	<p>P: ¿A nivel nacional como desempeñan sus actividades de I+D+i? R: Participamos <u>en convocatorias nacionales promovidas por los distintos ministerios y acudimos a la plataforma nacional de ciberseguridad e-SEC.</u> A través de esta plataforma he participado en alguna reunión telefónica, aunque la verdad es que <u>no existe actualmente mucha actividad a través de esta plataforma.</u> A nivel europeo hay muchas más actividades. <b>De acuerdo a su respuesta se amplía la pregunta:</b> P: ¿La manera en que se definen las necesidades de los proyectos o se ejecutan las actividades en esta plataforma cuentan con algún sistema de gestión de la calidad orientado a la excelencia? R: <u>No.</u></p>	<p>Facultades del ecosistema.</p> <p>Facultades del ecosistema</p>	<p>El entrevistado describe sus prácticas a nivel nacional sobre sus procesos I+D+i destacando la poca actividad que actualmente se lleva a cabo.</p> <p>El entrevistado manifiesta la poca participación en el establecimiento de los objetivos a conseguir con los procesos de I+D+i promovidos en el ámbito nacional.</p>
2E	<p>P: ¿A nivel internacional como desempeñan sus actividades? R: En Europa hay un programa de trabajo denominado “secure societies”. Este se puede ver como un plan I+D+i porque recoge las convocatorias para los retos a alcanzar en los próximos 2 o 3 años y las prioridades van</p>	<p>Facultades del ecosistema.</p>	<p>El entrevistado describe el contexto europeo en actividades I+D+i manifestando su capacidad de participación en estas iniciativas.</p>

	<p>definidas por las Comisión Europea. Sin embargo, este plan no solo considera la ciberseguridad, ya que incluye áreas como transporte e industria 4.0.</p> <p><b><u>Es importante dejar claro que con la figura ECSO se ha logrado integrar las acciones publico-privadas para atender los retos en ciberseguridad propuestos en el programa de trabajo Horizon 2020.</u></b></p>		
<b>No. preguntas:</b>	<b>4. Análisis del contexto actual del ecosistema de ciberseguridad en España dentro del marco I+D+i.</b>	<b>Categoría:</b>	<b>Sub - Categoría:</b>
4A	<p>P: ¿Considera usted que actualmente existe la necesidad de implementar un sistema de gestión de la calidad total en el ecosistema de ciberseguridad en España dentro del marco I+D+i?</p> <p>R: <b><u>En cualquier proceso siempre será importante promover la implementación de sistemas de gestión de la calidad</u></b>, lo que no tengo claro es si en los procesos I+D+i hace falta un sistema de gestión de la calidad concreto para el área de ciberseguridad.</p> <p><b>De acuerdo a su respuesta se amplía la pregunta:</b></p> <p>P: En distintas organizaciones a nivel internacional orientadas al R&amp;D, si se implementa un sistema de gestión de calidad total orientado a la excelencia, en donde las necesidades de los diversos agentes que conforman</p>	Necesidad del modelo.	El entrevistado deja clara la necesidad de un sistema de gestión de la calidad total.

	<p>esa organización son canalizadas y los proyectos son concebidos en función de estas necesidades detectadas. Incluso, esta misma metodología busca alcanzar la innovación hasta en aquellos procesos recurrentes y continuos. Ante esta posibilidad, ¿Considera usted que el ecosistema de ciberseguridad de España dentro del marco de I+D+i cuenta con las capacidades para implementar un sistema de calidad total?</p> <p>R: <b>Si.</b> Sin embargo, el sistema de gestión de calidad I+D+i implementado en la organización a la que represento incluye una serie de procedimientos que están basados en la aplicación de la norma antes mencionada y eso se podría resumir como una serie de pasos a seguir para llevar la gestión de proyectos I+D+i y esta metodología de trabajo al ser sinónimo de calidad, es un requisito para la obtención de financiación de proyectos.</p>	Facultades del ecosistema.	El entrevistado manifiesta que el ecosistema posee las facultades para implementar un sistema de calidad total.
<b>No. preguntas:</b>	<b>Retos por venir al ecosistema de ciberseguridad de España en el marco I+D+i.</b>	<b>Categoría:</b>	<b>Sub - Categoría:</b>
5A	<p>P: ¿Cuáles son los retos presentes en el ecosistema de ciberseguridad de España dentro del marco de I+D+i desde su perspectiva?</p> <p>R: El mayor reto presente en la Red es el de <b>definir un ecosistema entendible para los diversos actores que lo</b></p>	Facultades del ecosistema.	El entrevistado declara la falta de integración por parte

	<p><b>conforman</b>, ya que existen muchas organizaciones tanto públicas como privadas que buscan liderar este ecosistema lo que le hace ver como desarticulado.</p> <p>Incluso, se podría cuestionar que es el ecosistema, ya que se conocen algunas de estas organizaciones y de algunas plataformas que, como he mencionado, cuentan con poca actividad. Además del INCIBE y el RENIC el cual me comentas en esta entrevista, no hay mucho más que resaltar de este ecosistema.</p> <p><b>Es clara la necesidad de un referente</b>, ya que si yo quisiera hablar sobre proyectos I+D+i orientados a la ciberseguridad en España, no sabría a quién ir. A nivel europeo está mucho más claro. Además, a nivel nacional hay muy poca actividad.</p>	<p>Capacidades del RENIC.</p>	<p>de los agentes pertenecientes al ecosistema.</p> <p>El entrevistado manifestó la falta de liderazgo en el ecosistema, dejando en evidencia la falta del RENIC en esta función.</p>
<p>5B</p>	<p>P: ¿Conoce usted algún plan específico de ciberseguridad dentro del marco I+D+i?</p> <p>R: <b>No. Está recogido dentro de las líneas de acción a desarrollar de acuerdo a la ECN, pero no ha sido establecido aún.</b></p> <p>De acuerdo a su respuesta se amplía la pregunta</p> <p>P: ¿Y considera usted esto una carencia?</p> <p>R: No necesariamente, ya que esto se volverá necesario o no en función de cómo se organice la</p>		

	<p>Red. Me explico, <b><u>los procesos I+D+i pueden ser tanto horizontales como verticales permitiéndote esto desarrollar conocimientos tanto por sectores como por tecnologías y al ser la ciberseguridad una temática que abarca muchas áreas de conocimiento se podría coaccionar el alcance de estos desarrollos si se considerase un plan específico.</u></b></p> <p>A nivel europeo esta ha sido solucionado a través de los retos “secure societies” propuestos por medio del programa de trabajo Horizon 2020. Estos retos consideran el enfoque vertical con los retos “enabling technologies” y el enfoque horizontal a través de los retos “social networks”</p>	<p>Capacidades del RENIC.</p>	<p>El entrevistado, a pesar de desconocer al RENIC, al describir el funcionamiento de los procesos I+D+I promovidos a nivel continental, describió las bases sobre las que se soporta el modelado de la red bajo el constructo nodal, dejando en evidencia así las capacidades del RENIC bajo este modelado para desarrollar este tipo de procesos.</p>
--	---	-------------------------------	---

**Importante:**

- Fueron excluidas las preguntas que buscaban establecer conocimientos comunes asociadas a los objetivos estratégicos y a la conformación del RENIC por ser desconocida esta institución por el especialista entrevistado.
- Fueron excluidas las preguntas asociadas a los conceptos fundamentales de la excelencia propuestos por el modelo EFQM por ser desconocidas por el especialista entrevistado.

**Discusión de los resultados**

Los resultados obtenidos de la entrevista realizada reflejan varios elementos que podrían ser de relevancia para la investigación, que van desde la poca importancia que representa el RENIC y sus actuales acciones desde los diferentes entornos en los cuales el agente contactado desarrolla sus procesos I+D+i, hasta la admisión de una gran desconexión del agente consultado con el funcionamiento del resto del ecosistema. Sin embargo, al ser considerado solo un experto para la realización de esta actividad, se asume que estos datos son demasiado aislados para poder ser asumidos como constantes en todos los agentes del sector industrial que pertenecen al ecosistema. Pero esta limitación no restringe la detección, desde la perspectiva del consultado, de la necesidad de un modelo de excelencia EFQM, además de su apreciación sobre las capacidades tanto del RENIC para liderar este modelo como del ecosistema para llevar a cabo dicha implementación. Ante esto, el entrevistado manifestó las siguientes posturas:

De acuerdo con la información obtenida del experto, la necesidad de implementar un modelo de excelencia EFQM se hace presente durante toda la entrevista, destacándose la recomendación de promover la implementación de sistemas de gestión de la calidad en todos los procesos con especial atención a los procesos I+D+i (Pregunta 4A). Así mismo, en muchas de las aportaciones del experto se reflejan carencias tanto de los agentes como en el RENIC, que podrían

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

ser canalizadas con la implementación de dicho modelo, justificando de esta manera, la necesidad de su implementación.

Así mismo, en lo relativo a las facultades del RENIC para liderar la implementación del modelo en el ecosistema, la opinión del experto se vio claramente condicionada por la falta de información sobre el RENIC, llamando la atención el desconocimiento del experto de esta organización a pesar de haber pertenecido a los agentes consultados en la elaboración del estudio realizado por el INCIBE (2015). Siendo oportuno resaltar, que tanto la organización a la que pertenece el experto como el RENIC participan en la ECSO como miembros fundadores. Sin embargo, en el análisis en profundidad de la entrevista se puede destacar opiniones del experto que realzan las facultades del RENIC para liderar la implementación de un sistema de calidad total en el ecosistema de ciberseguridad español dentro del marco I+D+i. La pregunta 5B refleja como el entrevistado, al describir y aprobar la metodología de desarrollo de los procesos I+D+i a nivel continental, avala el modelado mixto que el RENIC propone para liderar en la red.

De igual manera, el entrevistado deja ver carencias en el RENIC que deberán ser tratadas y mejoradas para lograr desempeñarse como el líder que necesita la red. Estas oportunidades de mejora detectadas son la falta de liderazgo por parte del RENIC además de la poca difusión del RENIC como figura líder en el ecosistema, la falta de canales de comunicación abiertos con todos los agentes pertenecientes al ecosistema y la falta de iniciativas de procesos I+D+i a nivel nacional. Es importante acotar que más adelante en este capítulo se presenta una propuesta con la cual se busca canalizar todas estas oportunidades de mejora mediante la implementación de un modelo parcial de excelencia EFQM.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

Finalmente, al analizar la entrevista a profundidad se detecta la opinión del experto sobre el ecosistema de ciberseguridad en España, destacándose la pregunta 4A en la cual declara que si se poseen las facultades para llevar a cabo la implantación de un sistema de gestión de la calidad total. Es importante señalar que debido al desconocimiento del modelo EFQM por parte del entrevistado fueron retiradas durante la realización de la entrevista, las preguntas que destacaban los atributos del modelo. Sin embargo, esta limitación fue compensada con preguntas relacionadas sobre los conocimientos de gestión de la calidad y de procesos I+D+i.

Ante este escenario, resulta oportuno contrastar los resultados complementarios obtenidos a través de la aplicación de estas técnicas de recolección de datos con las posturas que proponen los teóricos consultados en esta investigación, desprendiéndose de este ejercicio las siguientes conclusiones:

- Se evidencia la falta de conexión del RENIC con los objetivos de sus agentes, tanto hacia el sector académico como con el industrial, también evidenciándose la poca difusión de las acciones realizadas desde su instauración. Ante esto, el modelo EFQM, según Calvo-Mora et al. (2016), se propone como un sistema de calidad total que permite la detección y el control de indicadores de desempeño en los procesos de todos los agentes involucrados a la organización. Logrando así, medir los resultados de estas acciones desde las perspectivas de los clientes, personas, sociedad, así como los resultados claves.
- Se ha podido establecerse que el RENIC no posee ningún canal de comunicación con sus agentes que le permita detectar sus necesidades o difundir las acciones

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

específicas derivadas de sus objetivos planteados. Esto se traduce en una inexistente iniciativa por parte del RENIC para añadir valor al funcionamiento del ecosistema aglutinando las necesidades, expectativas y oportunidades de sus agentes. Ante esto, el modelo EFQM se presenta como una opción para integrar los diversos agentes del ecosistema, y no solo eso, además plantea una serie de criterios interconectados para la organización. Logrando a través de estos criterios la realización de evaluaciones continuas de los objetivos estratégicos, tanto de manera horizontal como de manera vertical (Moreno, 2007).

- Ha quedado en manifiesto como carencia presente en el ecosistema objeto del estudio, la inexistencia de procedimientos que permitan medir el desempeño de los agentes que lo conforman en función de los objetivos que el RENIC ha establecido. En este sentido, Ghodousi & Mansouri (2016) plantean que el concepto fundamental “*Managing with agility*” se refleja principalmente en el modelo EFQM a través de la detección de oportunidades y necesidades sobre cada uno de los agentes facilitadores, presentes en la organización, desarrollando para esto instrumentos de comunicación periódica que permitan monitorizar y medir la evolución de la organización.
- Se refleja, tanto desde la perspectiva del sector académico como del industrial, la inexistencia de acciones concretas que promuevan el actual desempeño del ecosistema, así como la ausencia de controles de mejora continua a estas acciones. El modelo EFQM, según (Moreno, 2007), plantea que la excelencia se obtiene a

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

través de la constante evaluación de los resultados obtenidos (personas, clientes, sociedad y desempeño clave), siendo por esto tan importante la participación de todos los agentes involucrados en la organización en la definición de los indicadores de gestión. De igual manera, Trott (2009) plantea que a través del modelo EFQM se pueden lograr innovaciones sobre procesos continuos basados en la retroalimentación, producto de la interacción de los agentes de la organización. Pudiendo ser esta práctica, la solución para la dispersión de conocimiento evidenciada en el diagnóstico presentado por el INCIBE (2015).

Al resumir los resultados obtenidos se puede reseñar que, tanto para el sector académico como para la industria, existe la necesidad en el ecosistema de ciberseguridad de España de contar con una metodología de trabajo que busque mejorar continuamente el funcionamiento de la RED I+D+i, integrando los procesos de los agentes que la conforman y promoviendo el desarrollo integral de todo el ecosistema, a través de acciones inclusivas en donde sea considerada de manera constante la diversidad de roles, la gran variedad de actividades inherentes a sus procesos y la evolución constante de los sectores TIC, Ciberseguridad e I+D+i.

### **4.3 Conclusiones**

En este apartado, se busca satisfacer las interrogantes planteadas que motivaron el desarrollo de esta investigación. En este sentido, se puede concluir que:

En lo relación al primer objetivo específico, al intentar identificar la necesidad de un modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

dentro del marco I+D+i, se ha podido establecer que la necesidad está presente entre agentes de los sectores académico e industrial pertenecientes según la delimitación del ecosistema presentada por INCIBE (2015).

Así mismo, las actuales necesidades de la ciberseguridad, tanto nacional como internacionalmente, en lo relativo a soluciones (productos / servicios) innovadoras, indica ser este el momento propicio para llevar acciones de esta índole, buscando alcanzar y superar las exigencias que el constante desarrollo de las TIC representa con su acelerado ritmo de avance en áreas como el internet de las cosas (IoT), las ciudades inteligentes (Smartcities), entre otros (European Commission, 2016; Fischer, 2016; Jorgenson & Vu, 2016; Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012).

Seguidamente en referencia al segundo objetivo específico, al buscar determinar si el RENIC cuenta con las facultades necesarias para ejercer rol de líder en la implantación de un modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro del marco I+D+i, se puede establecer que sí dispone de las facultades para desarrollar su implementación. Esto obedece en gran medida a que su misión, visión y objetivos lo compromete a desempeñar el rol de líder en la RED, contando también con una posición privilegiada gracias al apoyo desde sus inicios del resto de agentes. Además, el que su marco de gobernanza, su misión, visión y objetivos sea el producto del consenso de opiniones de todos los agentes delimitados en el ecosistema por el INCIBE (2015) solo reafirma su capacidad como líder.

Adicionalmente, en relación al tercer objetivo específico, al buscar establecer la presencia de los requisitos del modelo parcial de excelencia EFQM para su implantación en el ecosistema

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

actual de la ciberseguridad en España dentro del marco I+D+i, se puede establecer que la RED sí dispone de las capacidades técnicas, organizativas y administrativas mínimas para lograr desarrollar de manera exitosa la implementación del modelo.

Finalmente, en cumplimiento al último objetivo específico propuesto, se presenta la propuesta del modelo EFQM que servirá de base para el desarrollo de su implantación en el ecosistema actual de ciberseguridad en España.

#### **4.4 Modelo parcial de excelencia EFQM para la ciberseguridad en España dentro del marco I+D+i.**

Como sucede con los SGC (sistemas para la gestión de la calidad), modelo de excelencia EFQM consta de un marco de trabajo, de no obligado cumplimiento, que desarrolla y realiza los conceptos de la calidad total y está orientado hacia la excelencia. EFQM es propiedad de la *European Foundation for Quality of Management* (EFQM), y se trata de un sistema generalista no vinculado a un sector o actividad concreta.

Los objetivos específicos que se espera lograr con esta propuesta son los siguientes:

1. Desarrollo de una herramienta eficaz para guiar al ecosistema de ciberseguridad en España en la auto-implantación de un SGC, con la referencia del Modelo EFQM de Excelencia.
2. Adaptación e interpretación del Modelo EFQM de excelencia a la realidad y características del ecosistema de ciberseguridad en España dentro del marco I+D+i.
3. Facilitar la hoja REDER como herramienta auxiliar útil para la implantación del modelo parcial de excelencia EFQM en el ecosistema de ciberseguridad en España dentro del marco I+D+i.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

Es importante tener en cuenta que esta propuesta se encuentra en un estado de desarrollo incipiente y que debe madurar con las aportaciones de los distintos agentes pertenecientes al ecosistema. Así mismo, deberá ser complementada con otros textos y conocimientos para su correcta aplicación, ya que lo que aquí se propone es una metodología aplicable a la práctica de la implantación de un SGC, existiendo unos temas previos que no son objeto de esta propuesta. En concreto, se hace referencia a una formación básica en gestión de la calidad (principios, identidad corporativa, política y estrategia, gestión por procesos, indicadores, etc.) y conocimientos del Modelo EFQM de Excelencia.

En cuanto al contenido de la propuesta, se ha estructurado de acuerdo con la metodología de intervención propuesta por Moreno (2007), en concreto se trabaja el proceso de autoevaluación y el de desarrollo de planes de acción para la mejora. Así mismo, se considera pertinente incluir un desarrollo previo que aborde la interpretación del Modelo EFQM de Excelencia desde la perspectiva del ecosistema de ciberseguridad en España, ya que los criterios para la interpretación del modelo son transversales y serán aplicados constantemente en todas las fases del proceso.

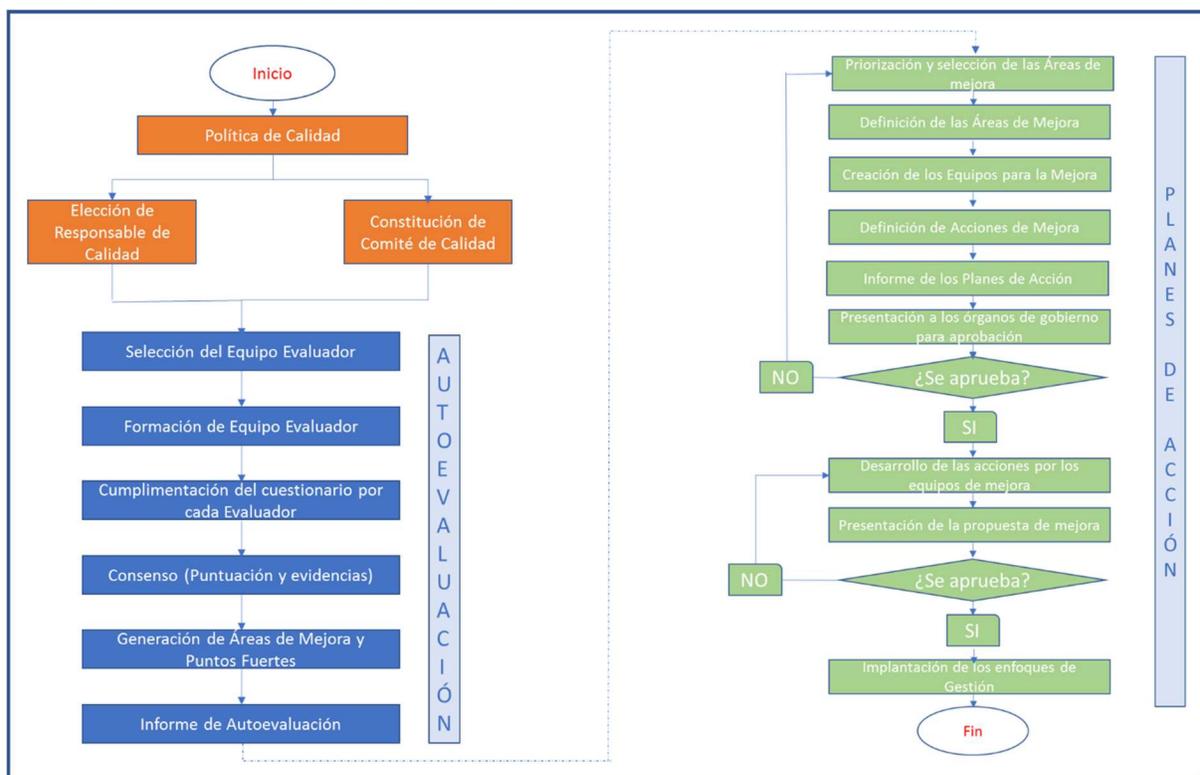
Es importante reiterar que el modelo propuesto se establece como parcial por considerar solo los objetivos estratégicos del RENIC bajo el enfoque nodal por su orientación a la excelencia. Así mismo, el liderazgo de esta propuesta será atribuido en gran medida al RENIC en virtud del resultado obtenido del segundo objetivo trazado, además de por lo establecido por INCIBE (2015).

**Metodología de intervención:**

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

La metodología de intervención propuesta para la aplicación del Modelo Parcial de Excelencia EFQM para la Ciberseguridad en España dentro del marco I+D+i se ha dividido en dos fases, la primera de ellas referida al proceso de autoevaluación, ya descrita previamente, y la segunda al proceso de planes de acción de mejora. Esta división obedece en gran medida a que en el ciclo de la mejora continua éstas figuran como fases independientes, en concreto evaluación (*check*) y mejora (*action*).



**Ilustración 7. Diagrama de metodología de intervención. Fuente: Moreno (2007).**

Como se puede observar en la ilustración 7, además de la 1ª fase (actividades en azul) y 2ª fase (actividades en verde), se han identificado unas fases previas necesarias (actividades en

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

naranja) y que no tienen por qué estar vinculadas al proceso de autoevaluación y planes de acción.

Estas actividades son:

- Definición de la política de calidad.
- Elección del responsable de calidad.
- Constitución del comité de calidad.

Estos elementos o equipos deben tener un carácter de permanencia en el tiempo que vaya más allá de la acción puntual de la autoevaluación y definición de los planes de acción. Es por esto que se deberá tener en cuenta el contexto actual de ciberseguridad en España dentro del marco I+D+i y la misión, visión y objetivos que el RENIC se plantea como líder de esta organización, ya que estas actividades tienen como objetivos:

- Formalizar públicamente las motivaciones y objetivos de la organización en materia de calidad.
- Dar coherencia al proceso.
- Establecer criterios, objetivos y herramientas a utilizar.
- Supervisar, dinamizar, coordinar y gestionar el proceso.

Así mismo, esta fase a pesar de ser previa posee gran trascendencia en el desarrollo del modelo parcial, ya que la definición de la política de calidad y la constitución del comité marcan los hitos a seguir sobre la definición de los indicadores de gestión. Además, el lograr diversidad de participación por parte de los agentes en esta fase permite la integración de sus necesidades y objetivos en las bases de medición que se plantea el modelo. El RENIC deberá jugar un rol integrador en esta fase, sin menospreciar las labores que se exigen en este punto al Polo tecnológico

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

de ciberseguridad de España, al INCIBE, al Centro Criptológico Nacional, a las Administraciones Públicas, a los centros universitarios y otros. Todos deberán participar en el debate donde se discuta y decida la política de calidad a implementar. La importancia de la participación radica en gran medida en la búsqueda de unificación de criterios al delimitar los resultados del modelo, habiendo sido resaltado por todos los autores consultados la conveniencia de incluir en esta fase a toda la organización.

Duración del proceso:

Es evidente que en un proceso de este tipo se podría determinar cuándo comienza pero difícilmente determinar cuándo concluye, ya que se trata de un trabajo que nunca termina, de un proceso que no tiene fin. Esta afirmación toma más énfasis si el Sistema de Gestión de la Calidad que se busca implantar se basa en los principios de la calidad total, de la mejora continua y además está orientado hacia la excelencia, como es el caso del Modelo EFQM.

En cuanto a la duración de los procesos ya mencionados, la autoevaluación (fase 1ª) y los planes de acción de mejora (fase 2ª), se podrá aproximar más su estimación partiendo de la experiencia, aunque será en cualquier caso muy subjetiva ya que las variables que lo determinan tendrán que ser definidas individual y puntualmente por cada agente participante. En cualquier caso, lo que sí manifiesta es la necesidad de realizar una planificación de las tareas y tiempos para la ejecución de ambas fases.

Las variables fundamentales a considerar para realizar esta planificación son las siguientes:

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

- Número de personas implicadas en el proceso formando parte de los diferentes equipos.
- Dedicación temporal y formación en calidad de los participantes.
- Disponibilidad de asesoramiento externo.
- Objetivos fijados por los agentes del ecosistema en términos de grado de implantación del sistema de gestión de la calidad, lo que determinará el alcance de los planes de mejora.
- Desarrollo actual del ecosistema de ciberseguridad en España dentro del marco I+D+i.

**Interpretación del Modelo parcial desde la perspectiva de la ciberseguridad en España dentro del marco I+D+i.**

En este apartado se busca unificar criterios sobre ciertos conocimientos del Modelo EFQM necesarios para poder llevar a cabo la implantación.

Interpretaciones transversales:

Al tratarse de un sistema generalista no vinculado a un sector concreto o actividad, es necesario repasar algunas cuestiones transversales del modelo; ya que a lo largo del desarrollo de la propuesta serán consideradas para cada criterio desde la perspectiva de la ciberseguridad en España. Además, dada la diversidad de agentes participantes, es conveniente unificar el significado de algunos conceptos básicos entre todos los miembros del ecosistema.

Benchmarking: es una práctica aplicable a la ciberseguridad en España, no solo por sus ventajas y aportaciones sino por los valores, principios y objetivos comunes que caracterizan, o

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

deberían caracterizar a este sector. Las mejoras a través del benchmarking, bien aplicado, suele ser significativa ya que se trata de buenas prácticas contrastadas y con recorrido.

Cientes: La consideración en el modelo del concepto cliente pasa por extender el concepto como el usuario directo, usuario indirecto, beneficiario, receptor del servicio, organización que contrata el servicio, etc. Es decir, cualquier personas físicas o jurídicas receptoras, directa o indirectamente, de los servicios o productos suministrados, independientemente de que haya o no una contraprestación económica o una solicitud o demanda previa del servicio o producto.

Competidor: Los competidores a los que se refiere el modelo, y que se deben considerar para su análisis, serán aquellas organizaciones del ecosistema con las que se comparta actividad, ya sea porque presten los mismos servicios o porque opten a los mismos recursos, tanto económicos, como técnicos y humanos.

Grupos de interés: Se trata de todos aquellos colectivos interesados por la organización, que interactúan directa o indirectamente, en cualquiera de las formas posibles de relación e independientemente del grado o medida de esa relación. En este punto deberá considerarse a todos los agentes del ecosistema.

Herramienta de análisis del modelo (Matriz de puntuación REDER)

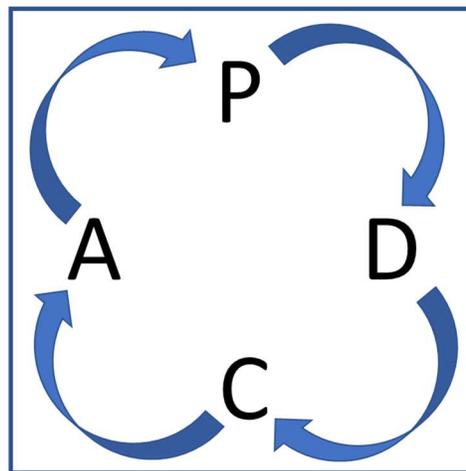
De acuerdo a lo planteado por EFQM (2012), el motor de análisis empleado en la autoevaluación que subyace en el modelo se basa en los cuatro elementos que corresponden al ciclo PDCA. Este concepto establece que una organización necesita:

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

P (plan): Planificar y desarrollar una sólida metodología para producir los resultados requeridos, tanto ahora como en el futuro, basándose en una mentalidad innovadora.

D (do): Implantar la metodología de un modo sistemático para garantizar su plena y efectiva puesta en práctica, alineando el despliegue del método, uno tras otro, cuando así proceda.



C (check): Evaluar la eficiencia y eficacia del método formulado y la implantación, con base en un seguimiento y un análisis de los resultados (indicadores) conseguidos y en actividades de indagación tales como las valoraciones comparativas y las evaluaciones.

A (act): Valorando esta información, identificar, jerarquizar, planificar y llevar a la práctica las mejoras que resulten necesarias.

El modelo EFQM proporciona la herramienta para que sean analizados estos cuatro elementos en cada práctica de gestión propuesta a lo largo de sus criterios y subcriterios. Esta herramienta denominada REDER (Moreno, 2007), permite llevar a cabo la autoevaluación descrita en el capítulo II. Este acrónimo representa las siglas de los siguientes conceptos: Resultados, Enfoque, Despliegue, Evaluación y Revisión.

Resultados: Son los resultados deseados por la organización en sus diferentes áreas de gestión. Estos resultados son en realidad los indicadores que se utilizarán para medir la excelencia de las prácticas de gestión planificadas y desplegadas por la organización.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

Enfoque: Se refiere a la fase de planificación. El enfoque es la etapa en la que se definen los procesos necesarios para realizar el trabajo y donde se va a realizar. Estos procesos deben estar claramente definidos y tener en cuenta las informaciones o resultados de otras áreas de la organización para desarrollarse de manera eficaz.

Despliegue: Se trata de la puesta en práctica de los procesos definidos en el enfoque. La aplicación de los procesos, definidos de un modo sistemático, refuerza las políticas y estrategias de la organización en su aplicación día a día.

Evaluación: Se refiere a la medición de los resultados obtenidos de los procesos definidos y su aplicación, con orientación hacia la excelencia esperada de los indicadores establecidos.

Revisión: Fruto de la revisión de las mediciones efectuadas, tienen lugar las actividades de aprendizaje con las que se busca identificar, jerarquizar, planificar y poner en práctica las acciones de mejora.

Como se aprecia, REDER se refiere a los mismos conceptos presentes en la autoevaluación descrita en el apartado 2.6, la única diferencia es que se añade la necesidad de disponer de unos resultados o indicadores para realizar la evaluación correspondiente. En este sentido, durante el desarrollo la hoja REDER deberán ser analizados desde varias perspectivas los agentes facilitadores del modelo (criterios 1 a 5). Estas perspectivas son: su enfoque, su forma de desplegarlo, y la manera de evaluarlo y revisarlo. A su vez, para evaluar cada una de estas perspectivas, la hoja REDER propone centrar el análisis en varios conceptos. En este sentido, a continuación se ilustran unas matrices de rubricas de la aplicación de las métricas para guiar a los evaluadores:

Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en

España dentro de un marco I+D+i

Victor E. Vera Pinto

Elementos	Atributos	0%	25%	50%	75%	100%
Enfoque	Sólidamente fundamentado: - El enfoque tiene una lógica clara - El enfoque a definido los procesos El enfoque se centra en las necesidades de los grupos de interés	Sin evidencia	Alguna evidencia	Evidencia	Evidencia clara	Evidencia total
	Integrado: - El enfoque apoya la política y la estrategia - El enfoque está vinculado a otros enfoques cuando procede	Sin evidencia	Alguna evidencia	Evidencia	Evidencia clara	Evidencia total
	Total	0 5 10	15 20 25 30 35	40 45 50 55 60	65 70 75 80 85	90 95 100
Elementos	Atributos	0%	25%	50%	75%	100%
Despliegue	Implantado: - El enfoque está implantado	Sin evidencia	Implantado en ¼ de las áreas relevantes	Implantado en ½ de las áreas relevantes	Implantado en ¾ de las áreas relevantes	Implementado en todas las áreas relevantes
	Sistemático: - El enfoque está desplegado de manera estructurada, habiéndose planificado y ejecutado de manera coherente el método utilizado para el despliegue	Sin evidencia	Alguna evidencia	Evidencia	Evidencia clara	Evidencia total
	Total	0 5 10	15 20 25 30 35	40 45 50 55 60	65 70 75 80 85	90 95 100
Elementos	Atributos	0%	25%	50%	75%	100%
Evaluación y revisión	Medición: - Se mide regularmente la eficacia del enfoque y del despliegue	Sin evidencia	Alguna evidencia	Evidencia	Evidencia clara	Evidencia total
	Aprendizaje: - Se utiliza para identificar mejores prácticas y oportunidades de Mejora	Sin evidencia	Alguna evidencia	Evidencia	Evidencia clara	Evidencia total
	Mejora: - Las mediciones y actividades de aprendizaje se analizan y utilizan para identificar, establecer prioridades, planificar e implantar mejoras	Sin evidencia	Alguna evidencia	Evidencia	Evidencia clara	Evidencia total
	Total	0 5 10	15 20 25 30 35	40 45 50 55 60	65 70 75 80 85	90 95 100
<b>Valoración total</b>		0 5 10	15 20 25 30 35	40 45 50 55 60	65 70 75 80 85	90 95 100

Tabla 7. Hoja REDER Criterio facilitadores. Fuente: Moreno (2007).

De igual manera, los criterios resultados deben ser analizados desde diferentes perspectivas al igual que los agentes facilitadores. Estas perspectivas son: sus tendencias, sus objetivos, las comparaciones, sus causas y su ámbito de aplicación. A continuación, se expone el significado de cada una de éstas.

Elementos	Atributos	0%	25%	50%	75%	100%
Resultados	Tendencias: -Las tendencias son positivas y/o -El rendimiento es bueno y sostenido	Sin resultados	Tendencias positivas y/o rendimiento satisfactorio en aproximadamente ¼ de	Tendencias positivas y/o rendimiento satisfactorio en aproximadamente ½ de los resultados	Tendencias positivas y/o rendimiento satisfactorio en aproximadamente 3 / 4 de los resultados	Tendencias positivas y/o rendimiento satisfactorio en todos los

Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en

España dentro de un marco I+D+i

Victor E. Vera Pinto

			los resultados durante al menos 3 años	durante al menos 3 años	durante al menos 3 años	resultados durante al menos 3 años
	Objetivos: - Los objetivos se alcanzan - Los objetivos son adecuados	Sin resultados	Alcanzados y adecuados en aproximadamente ¼ de los resultados	Alcanzados y adecuados en aproximadamente ½ de los resultados	Alcanzados y adecuados en aproximadamente ¾ de los resultados	Alcanzados y adecuados en todos los resultados
	Comparaciones: - Los resultados son buenos comparados con otros - Los resultados son buenos comparados con el reconocido como “el mejor”	Sin resultados	Comparaciones favorables en aproximadamente ¼ de los resultados	Comparaciones favorables en aproximadamente ½ de los resultados	Comparaciones favorables en aproximadamente ¾ de los resultados	Comparaciones favorables en todos los resultados
	Causas: - Los resultados son consecuencia del enfoque	Sin resultados	La relación causa/efecto es visible en aproximadamente ¼ de los resultados	La relación causa / efecto es visible en aproximadamente ½ de los resultados	La relación causa/efecto es visible en aproximadamente ¾ de los resultados	La relación causa/efecto es visible en todos los resultados
	Total	0 5 10	15 20 25 30 35	40 45 50 55 60	65 70 75 80 85	90 95 100
<b>Alcance</b>	<b>Atributos</b>	<b>0%</b>	<b>25%</b>	<b>50%</b>	<b>75%</b>	<b>100%</b>
Despliegue	Ámbito de aplicación: - Los resultados abarcan las áreas relevantes - Los resultados se segmentan adecuadamente, p.e. por cliente, tipo de producto o servicio, área geográfica	Sin resultados o con información anecdótica	Los resultados abarcan ¼ de las áreas y actividades relevantes	Los resultados abarcan 1/2 de las áreas y actividades relevantes	Los resultados abarcan ¾ de las áreas y actividades relevantes	Los resultados abarcan todas las áreas y actividades relevantes
	Total	0 5 10	15 20 25 30 35	40 45 50 55 60	65 70 75 80 85	90 95 100
<b>Valoración total</b>		0 5 10	15 20 25 30 35	40 45 50 55 60	65 70 75 80 85	90 95 100

Tabla 8. Hoja REDER Criterios resultados. Fuente: Moreno (2007).

**Resultados:** Miden la excelencia y el ámbito de aplicación de lo que la organización aporta de valor a sus distintos grupos de interés y de los que la organización está alcanzando en términos de eficiencia y eficacia. Los logros alcanzados se miden en función de la percepción de los diferentes grupos de interés, los propios objetivos de la organización y las comparaciones externas a ella.

Cada una de las palabras “Tendencias”, “Objetivos”, “Comparaciones”, “Causa” y “Ámbito de aplicación” se refieren a la excelencia de los resultados presentados donde:

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

- Tendencias. En todos los criterios de resultados se presentan las “Tendencias” de los datos relativos a los diversos parámetros utilizados para medir los resultados de clientes, de personal entre otros, donde una tendencia positiva es aquella que muestra una mejoría general a lo largo del tiempo.
- Objetivos. Se refiere a las propias metas internas de la organización. Para cada tendencia de resultados presentada deberá especificarse el objetivo interno, además de la tendencia esperada a lo largo del tiempo.
- Comparaciones. Se refiere a las realizadas con organizaciones externas; promedios del sector, o bien organizaciones reconocidas como las “mejores en su clase”.

Es importante para el RENIC considerar que la información presentada en los criterios de resultados indique las razones que justifican los objetivos estratégicos fijados, de modo que pueda juzgarse si estos objetivos son estimulantes para el funcionamiento del ecosistema orientándolo hacia la excelencia. Así mismo, el RENIC deberá considerar para las comparaciones como el mejor de su clase a aquellas organizaciones internacionales que destaquen en el sector I+D+i en ciberseguridad. Esto obedece a la proyección global que se plantea en sus objetivos.

Ámbito de aplicación: Es el impacto que tienen los resultados y en que afectan las áreas relevantes. Es necesario dar los resultados de todos los agentes y sectores del ecosistema dentro del ámbito de la evaluación, y cubrir adecuadamente todas las facetas relevantes del criterio. Además, se debe tener en cuenta la calidad de la “segmentación” de los resultados manejados. Es decir, la capacidad de los resultados de representar a todos los públicos o partes interesadas importantes.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

Para llegar a formar un juicio sobre el “ámbito de aplicación” de los resultados, es preciso adoptar un punto de vista global sobre la organización objeto de evaluación. Por consiguiente, es necesario que se pongan de relieve las relaciones entre los resultados y los métodos descritos en los criterios facilitadores. En resumen, la autoevaluación deberá abordar los siguientes aspectos para cada criterio de evaluación:

**Resultados**

- ¿Qué resultados se han conseguido hasta la fecha? ¿Cuál es su tendencia?
- ¿Cuáles son los objetivos anteriores, actuales y futuros?
- ¿Cómo queda el desempeño del RENIC y del ecosistema en comparación con el de otras organizaciones?
- ¿Cuáles son las causas de los resultados y qué acción se han emprendido en vista de ello?
- ¿Los resultados son consecuencia de los enfoques?

Interpretación de criterios

Basado en lo propuesto por EFQM (2012), en el capítulo II (tabla 6) son expuestas las exceptivas por cada criterio facilitador que se espera alcanzar en cada objetivo estratégico nodal establecido por el RENIC. Sin embargo, para la interpretación de los criterios del modelo resulta necesario presentar el siguiente esquema de todos los criterios y subcriterios. Así mismo, se aclara que no se pretende hacer un análisis exhaustivo del modelo, sino destacar las principales características:

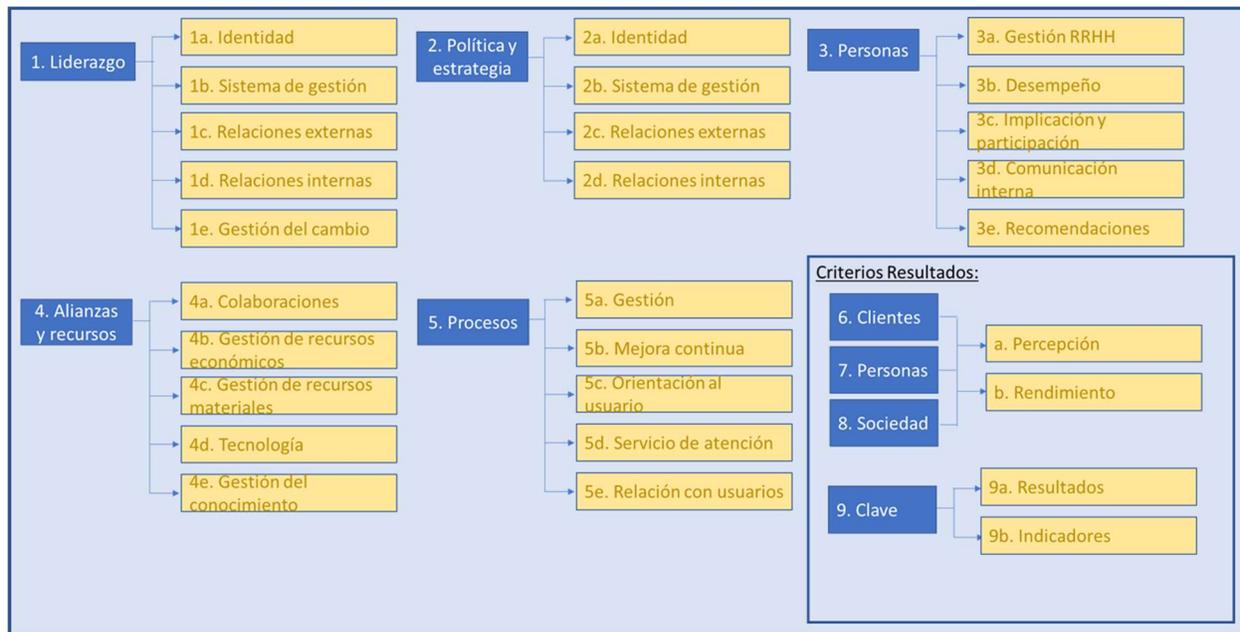


Ilustración 9. Criterios y subcriterios de modelo EFQM. Fuente: Elaboración propia.

Es importante tener presente que el modelo en su planteamiento inicial propone a las organizaciones un proceso o ciclo de mejora continua. Esto obedece a que, al establecer la línea de innovación y aprendizaje, EFQM está recomendando una continua revisión de los resultados obtenidos que facilite a las organizaciones el establecimiento de planes de mejora. A su vez, estos agentes facilitadores serán medidos y evaluados a través de los nuevos resultados obtenidos y el ciclo volverá a repetirse. Sin embargo, esta tarea requiere en primer lugar conocer y comprender qué dice EFQM.

El lenguaje empleado por el modelo, aplicable a todo tipo de organizaciones, hace que en muchas ocasiones no resulte fácil entender qué quiere decir el modelo en realidad, por lo que el comité de calidad deberá estar lo suficientemente capacitado para desarrollar el significado de cada

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

criterio y sus subcriterios correspondientes bajo la perspectiva del ecosistema de ciberseguridad español.

### Autoevaluación con ejes transversales

Mediante un análisis rápido de la estructura del modelo, se puede adivinar la existencia de una primera lectura transversal u horizontal obvia entre los criterios agentes y los criterios de resultados. Resulta fácil comprender que cuando se está analizando un criterio agente se debe analizar al mismo tiempo su criterio de resultados correspondiente. Por ejemplo, cuando se analiza el criterio 3 “Personas”, se deberá analizar al mismo tiempo el criterio 7 Resultados en las personas.

Por otro lado, es lógico pensar que como organización interesa conocer y analizar las interrelaciones y/o influencias que unos criterios tienen en otros. Por ejemplo, lo que una organización planifique y despliegue en un criterio como el 2 Política y estrategia, seguro que influirá en lo que la misma planifique y despliegue el criterio 5 Procesos, o en el 3 Personas. De la misma manera, lo que esta organización planifique y despliegue en un criterio como el 3 Personas, influirá a su vez en lo que se planifique y despliegue en el criterio 5 Procesos. Y así sucesivamente.

Esta lectura transversal ya no es tan obvia como la primera (entre criterios agentes y sus resultados), pero no por eso deja de ser una poderosa herramienta que la organización puede utilizar a la hora de definir relaciones horizontales. Incluso se puede (y se debe) ir más allá, y pasar a identificar las relaciones transversales que pueden existir entre subcriterios del modelo. Por ejemplo, se puede establecer que el 1b “Cómo los líderes se implican en el desarrollo y mejora del

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

sistema de gestión”, influye y está relacionado con el 3c “Sistemas de participación del personal”, y a su vez con el 5a “Diseño del sistema de gestión”, también con el 5b “Mejora del sistema de gestión” y con el 5e “Relaciones con los clientes”. A estas relaciones entre subcriterios del modelo las denominaremos “ejes transversales” o “ejes horizontales”.

La utilización de los ejes transversales permite analizar conceptos relevantes para la organización utilizando el modelo EFQM. Conceptos como la comunicación interna, la gestión y organización de procesos, la convivencia en la organización, la orientación al cliente o la mejora continua, son susceptibles de ser analizados de forma transversal con el modelo. Es decir, se puede identificar qué criterios y subcriterios del modelo EFQM se relacionan con el concepto elegido, realizando una selección horizontal de los mismos que comenzará en el criterio número uno, liderazgo y finalizará en el número nueve, Resultados clave. A continuación, se expone un ejemplo construyendo un eje transversal el cual se denominará “comunicación interna”.

La pregunta a realizarse será: ¿Qué criterios y subcriterios se relacionan con el eje “comunicación interna” a lo largo de todo el modelo parcial de excelencia EFQM para la ciberseguridad en España dentro del marco I+D+i?

En el ejemplo que se expone, se muestran las respuestas propuestas y las causas de la elección de las mismas.

Dentro del criterio número uno, liderazgo, el eje “comunicación interna” se relaciona con:  
1d Los líderes refuerzan una cultura de Excelencia entre las personas de la organización.

Dentro del criterio 2 Política y estrategia, el eje “comunicación interna” se relaciona con:  
2d La política y estrategia se comunica y despliega mediante un esquema de procesos clave.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

Dentro del criterio 3 Personas, el eje “comunicación interna” se relaciona con: 3d Existencia de un diálogo entre las personas y la organización.

Dentro del criterio 4 Alianzas y recursos, el eje “comunicación interna” se relaciona con: 4e Gestión de la información y del conocimiento.

Dentro del criterio 5 Procesos, el eje “comunicación interna” se relaciona con: 5b Introducción de las mejoras necesarias en los procesos mediante la innovación, a fin de satisfacer plenamente a clientes y otros grupos de interés, generando cada vez mayor valor.

El criterio 6 Resultados en los clientes, no tiene una relación directa con el eje “comunicación interna”, pues se refiere a mediciones relacionadas con los clientes y no a mediciones relacionadas con la comunicación interna.

Dentro del criterio 7 Resultados en las personas, el eje “comunicación interna” se relaciona con: 7a Medidas de percepción de las personas sobre la comunicación interna y 7b Indicadores de rendimiento de la comunicación interna.

El criterio 8 Resultados en la sociedad, no tiene una relación directa con el eje “comunicación interna”. Este criterio se refiere a las mediciones que puedo realizar del impacto del RENIC en la sociedad.

Dentro del criterio 9 Resultados clave, el eje “comunicación interna” se relaciona con: 9b Indicadores clave de rendimiento.

A continuación, se resumen las causas que justifican la relación del eje “comunicación interna” en el caso de estudio:

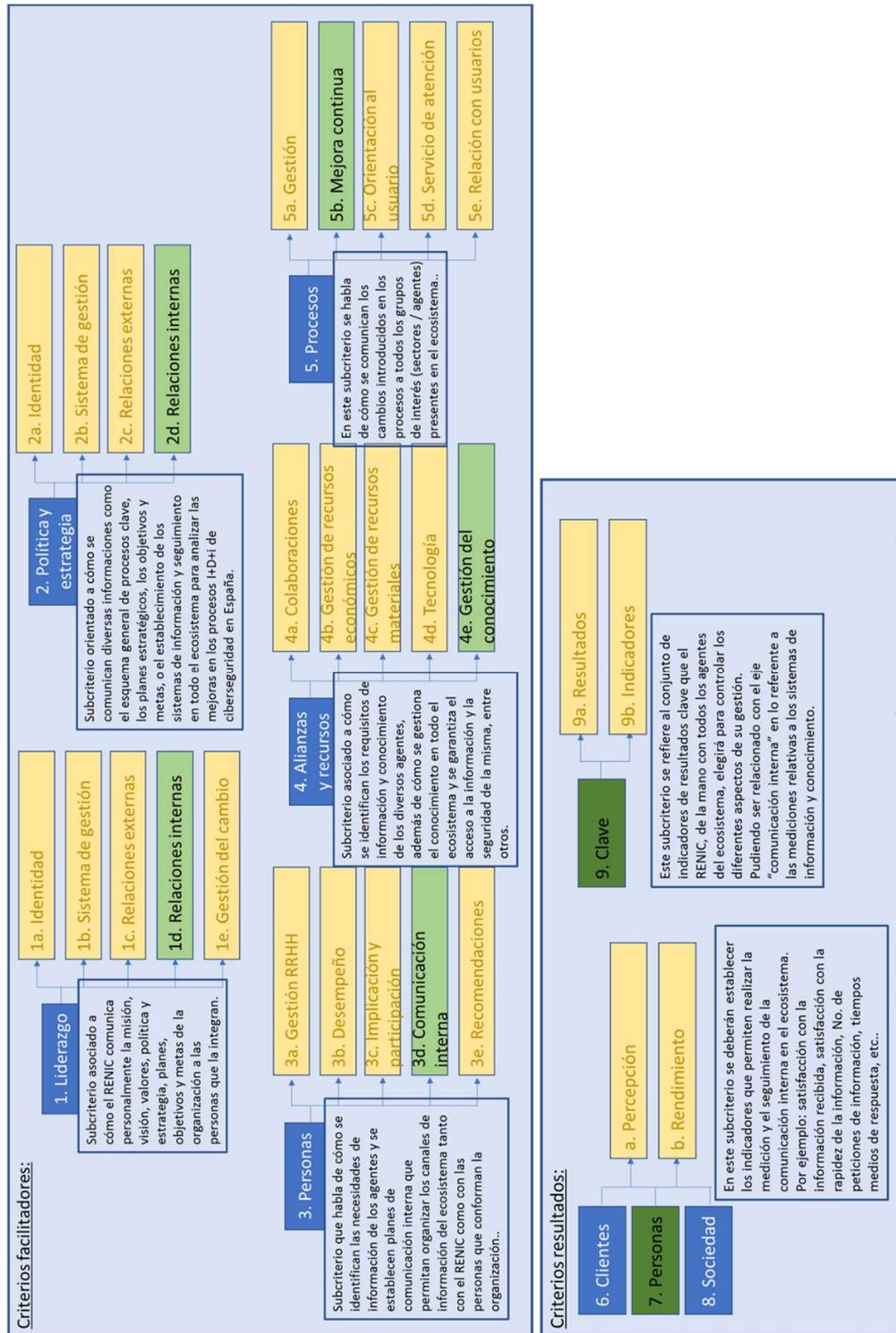


Ilustración 10. Causas de relación de subcriteros con eje "comunicación interna". Fuente: Elaboración propia.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

Por lo tanto, el eje “comunicación interna” estaría compuesto en este ejemplo por los subcriterios:

1d, 2d, 3d, 4e, 5b, 7a, 7b, 9b

Como se evidencia, se ha conseguido construir el eje transversal de la “comunicación interna” en el ecosistema de ciberseguridad en España, que permite analizar este concepto desde la perspectiva del liderazgo, de la política y estrategia, de las personas, de los recursos, de los procesos y de sus resultados relacionados. En otras palabras, se pueden identificar las áreas de mejora del liderazgo en relación al eje comunicación interna, las áreas de mejora de las políticas y estrategias en relación a este eje, las áreas de mejora en las personas, recursos, procesos, y por último, las áreas de mejora en los resultados relacionados con la comunicación interna.

Cada organización debe diseñar y crear sus propios ejes horizontales para así poder analizarlos. El ejemplo presentado podría incluir más subcriterios del modelo (como son el 1e ó el 4d), que también se relacionan con el eje “comunicación interna”. Las características de cada organización y su situación real ayudarán a elegir qué criterios y subcriterios son los que tienen que formar parte del eje transversal analizado.

### **Proceso de autoevaluación (Formularios con reuniones de trabajo)**

Para llevar a cabo el proceso de autoevaluación se proponen dos metodologías de las propuestas por EFQM (2012), que unidas permiten aprovechar todas las ventajas que ofrecen de

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

forma separada. Se trata del método de los formularios unido con el método de la reunión de trabajo.

Según Moreno (2007), realizar la autoevaluación de esta manera permite obtener los siguientes beneficios:

- Permite la recogida de los puntos fuertes y áreas de mejora.
- La autoevaluación se basa en la aportación de evidencias (datos y hechos) sobre los puntos fuertes y áreas de mejora.
- Ayuda a la comprensión del modelo por la dirección y refuerza el compromiso de implantación.
- La discusión y el consenso crean una visión común de la situación de la organización.
- Ayuda a difundir un lenguaje común “de la calidad” entre los miembros de la organización.
- Permite participar a gran cantidad de personas.
- La profundidad del análisis es muy elevada.
- Divide el trabajo de evaluación en equipos, permitiendo no sobrecargar de trabajo al personal de la organización.
- Permite poner en común diferentes puntos de vista y consensuar ideas.

A continuación, se describe el proceso a seguir para realizar una autoevaluación utilizando formularios y reuniones de trabajo.

### Elaborar los formularios

El primer paso de todos consiste en elaborar el formulario para analizar los criterios facilitadores y el formulario para analizar los criterios resultado. Como se muestra en los ejemplos siguientes presentados en la tabla 9, en ambos casos deberá incluirse los siguientes elementos comunes:

- El título del criterio y descripción.
- El título del subcriterio y su descripción.
- Las áreas a valorar.
- Puntos fuertes y áreas de mejora.
- Zona de puntuación: espacio reservado para indicar la puntuación que se estima oportuna para el subcriterio analizado. Para los subcriterios facilitadores existirá un espacio reservado para puntuar el enfoque, despliegue, evaluación y revisión, y el total. Para los subcriterios de resultados el espacio permitirá puntuar las tendencias, los objetivos, las comparaciones, las causas, el ámbito de aplicación y el total. A continuación, se muestran dos ejemplos de formularios donde el primero para un subcriterio facilitadores y el segundo para un subcriterio de resultados.

<b>Criterio 1: Liderazgo</b>			
Cómo los líderes desarrollan y facilitan la consecución de la misión y la visión, desarrollan los valores para alcanzar el éxito a largo plazo e implantan todo ello en la organización mediante las acciones y los comportamientos adecuados, estando implicados personalmente en asegurar que el sistema de gestión de la organización se desarrolla e implanta.			
<b>&lt;Subcriterio 1a</b>			
Desarrollo de la misión, visión y valores por parte de los líderes, que actúan como modelo de referencia dentro de una cultura de Excelencia			
<b>Áreas a valorar</b>		<b>Puntos fuertes</b>	
<ul style="list-style-type: none"> <li>• Desarrollar la misión y visión de la organización.</li> <li>• Desarrollar, actuando como modelo de referencia, los principios e ticos y valores de la organización.</li> <li>• Revisar y mejorar la efectividad de su propio liderazgo</li> <li>• Implicarse activa y personalmente en las actividades de mejora.</li> <li>• Estimular y animar la asunción de responsabilidades</li> <li>• Animar, apoyar y emprender acciones de mejora</li> <li>• Establecer prioridades entre las actividades de mejora.</li> <li>• Estimular y fomentar la colaboración dentro de la organización.</li> </ul>		<b>Áreas de mejora</b>	
<b>Enfoque</b>	<b>Despliegue</b>	<b>Evaluación y revisión</b>	<b>Total</b>

**Tabla 9. Modelo de formulario de subcriterio facilitadores. Fuente: Moreno (2007).**

<b>Criterio 6: Resultados en los clientes</b>					
Las organizaciones excelentes miden de manera exhaustiva y alcanzan resultados sobresalientes con respecto a sus clientes					
Subcriterio 6a					
Estas medidas se refieren a la percepción que tienen los clientes de la organización, (encuestas, grupos focales, clasificaciones de proveedores, felicitaciones y quejas)					
Áreas a valorar			Puntos fuertes		
LA IMAGEN GENERAL • Accesibilidad • Comunicación • Flexibilidad • Comportamiento proactivo • Capacidad de respuesta • Comparación con competencia		PRODUCTOS Y/O SERVICIOS • Calidad • Valor añadido • Fiabilidad • Innovación en el producto y/o servicio • Características de la entrega • Perfil medioambiental	Áreas de mejora		
VENTAS Y SERVICIO POSVENTA • Capacidad y conducta de las personas de la organización • Asesoramiento y apoyo • Publicaciones y documentación para los clientes • Tratamiento de quejas y reclamaciones • Formación o información sobre el producto • Tiempos de respuesta • Apoyo técnico		FIDELIDAD • Intención de continuar la relación con la organización • Voluntad de ampliar la relación con la organización usando otros productos y/o servicios de la misma • Voluntad de recomendar la organización			
Tendencias	Objetivos	Comparaciones	Causas	Ámbito de aplicación	Total

Tabla 10. Modelo de formulario de subcriterio resultados. Fuente: Moreno (2007).

### Definir los equipos de autoevaluación

Una vez elaborados los formularios, se deberán definir los diferentes equipos de evaluación. A continuación, se presentan algunas recomendaciones al respecto:

- La regla básica es: el equipo que evalúe un criterio o subcriterio debe tener información sobre lo que ocurre en la organización. Por ejemplo: el equipo que evalúe el criterio 3 (personas), deberá tener información sobre la gestión de los recursos humanos en su organización.

- Es recomendable que los equipos estén formados al menos por 3 personas como mínimo y 5 ó 6 como máximo para lograr diversidad en opiniones y postura, así como facilidad al momento de consensos.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

- Al equipo que evalúe un criterio agente determinado, es conveniente asignarle la evaluación del criterio resultado que se corresponda con ese agente. Es decir, si se evalúa el criterio 3 (personas), se deberá evaluar también el criterio 7 (resultados en las personas). De esta manera el equipo analizará cómo se planifican, se realizan y se miden las cosas, pero también qué resultados se obtiene con ellas.

- No es necesario que un equipo evalúe todos los criterios del modelo, sino la parte que le ha sido asignada. No obstante, todos los criterios del modelo deben ser evaluados.

- Mantener una reunión de lanzamiento con los equipos en la que se entregará el material y se indicarán los plazos de entrega de sus conclusiones. Es habitual dejar un periodo de 2 semanas para que cada miembro del equipo realice su autoevaluación individual.

### Realizar la autoevaluación individual

El primer trabajo del equipo consiste en que cada uno de sus miembros realice una reflexión individual utilizando los formularios suministrados. Esta evaluación individual debe concluir con la definición de los puntos fuertes, áreas de mejora y puntuación que se consideren oportunos. Para realizar la autoevaluación individual no sólo deberá utilizarse la hoja del formulario. Sino que también la matriz REDER debe acompañar en todo momento al evaluador como guión de análisis e identificación de puntos fuertes y áreas de mejora.

La identificación de puntos fuertes y áreas de mejora en los criterios agentes facilitadores y en los resultados es el gran objetivo de la autoevaluación de cualquier organización.

### Identificar puntos fuertes y áreas de mejora

A continuación, se describen los pasos a seguir en el proceso de análisis de un subcriterio facilitador. Este proceso nos debe ayudar a identificar puntos fuertes y áreas de mejora.

1. Leer el subcriterio que se pretende analizar e identificar claramente de qué se trata. Todo el personal implicado en el análisis de un subcriterio debe tener claro qué debe y qué no debe tener en cuenta a la hora de reflexionar sobre el.

2. Leer lo que el modelo propone como ejemplos de desarrollo o áreas a valorar (significa lo mismo), del subcriterio analizado.

3. Identificar la realización del área de aplicación de la organización (punto fuerte) o la no realización y no aplicación (área de mejora), de prácticas de gestión que pueden dar respuesta a los ejemplos que propone el modelo (recordemos que el modelo no es prescriptivo y se le puede dar respuesta de muchas maneras diferentes).

4. Redactar el punto fuerte o área de mejora, según se trate. Para la redacción de puntos fuertes y áreas de mejora, seguir las recomendaciones que más adelante se exponen.

5. Al llegar a este punto, se pueden tener ya identificadas bastantes áreas de mejora. Estas áreas de mejora indican únicamente si la organización realiza o no determinadas prácticas de gestión que dan respuesta a los conceptos propuestos por el modelo. Se debe recordar que para evaluar con profundidad la gestión en la organización, no sólo se debe analizar si hacemos o no algo. También se deberá analizar si se realiza de forma sistemática, si se planifica o no, si es medido o no, y si se mejora o no, revisando los resultados de esa medición. De esta manera, se evalúa la

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

capacidad de la organización para aprender y mejorar fruto de la revisión de los resultados obtenidos.

6. Revisión final: una vez finalizadas todas estas reflexiones, es recomendable revisar la hoja REDER de agentes facilitadores para verificar si se han identificado mejoras sobre planificación, ejecución, revisión.

Visto de otro modo, para valorar los agentes facilitadores se debe preguntar:

- ¿Qué hace (o no hace) el RENIC y los agentes presentes en el ecosistema para dar respuesta al criterio evaluado?
- ¿Tienen definidos los procesos para lo que hace la organización?
- ¿Se integra las actuaciones del RENIC y sus agentes con otras áreas del ecosistema dentro del marco I+D+i?
- ¿Se realizan los procesos tal y como están planificados? ¿Son ejecutados de forma sistemáticamente?
- ¿Se realiza la medición de los resultados de lo que se hace?
- ¿Hay aprendizaje del análisis de las mediciones realizadas y hay mejoras fruto de dichas mediciones?

Seguidamente se describe el proceso a seguir para identificar puntos fuertes y áreas de mejora en los resultados.

- Leer los resultados propuestos por el modelo para el subcriterio que se está analizando.
- Averiguar con qué indicadores cuenta la organización para medir las prácticas de gestión relacionadas con el subcriterio analizado.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

- Para estos indicadores existentes, definir puntos fuertes y áreas de mejora referentes a sus tendencias y objetivos.

- Asimismo, definir puntos fuertes y áreas de mejora para las causas que provocan estos indicadores y su ámbito de aplicación.

- Determinar que indicadores no están disponibles para medir las prácticas de gestión relacionadas con el subcriterio analizado. Incluir su obtención como área de mejora.

Desde otra perspectiva, para valorar los resultados se debe preguntar:

- ¿Qué indicadores se utilizan y cuáles no?
- ¿Existen tendencias positivas para los indicadores actuales?
- ¿Tienen objetivos asignados? ¿Se cumplen?
- ¿Se comparan? ¿Son mejores que los de la competencia?
- ¿Los procesos que los provocan están claros e identificados?
- ¿Son suficientes para medir lo que se hace? ¿Se segmentan?

Recomendaciones para la redacción:

- Redactar hechos y no opiniones.
- Toda afirmación debe ir acompañada de su justificación mediante hechos y no opiniones.
- No valorar los comportamientos, actitudes o actividades de las personas.
- Evaluar el subcriterio asignado evitando en todo momento evaluar aspectos que se incluyen en otros subcriterios cuando se esté evaluando.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

- Intentar que la descripción de la mejora se centre en temas concretos y no muy generales o abstractos.
- Verificar que las informaciones que se incluyen son hechos reales y verídicos.
- Redactar frases comprensibles y lógicas, de manera breve y concisa posible.
- Para valorar resultados centrarse en valorar sus tendencias, objetivos, comparaciones, causas y ámbito de aplicación.

### Puntuar agentes facilitadores y resultados

La puntuación en el proceso de autoevaluación tiene una regla básica que en todo momento se debe cumplir: se puntúa siempre después de haber identificado los puntos fuertes y áreas de mejora. Intentar puntuar antes de identificar los mencionados puntos fuertes y áreas de mejora no es más que un ejercicio de intuición subjetivo, que no lleva a ninguna conclusión fundamentada en la realidad. Por eso la puntuación mediante cuestionario no es del todo realista.

El proceso de puntuación, para ser coherente y no desviarse demasiado de la realidad, podría ser realizado siguiendo los pasos siguientes. En cualquier caso, siempre deberían utilizarse las matrices de puntuación para agentes y resultados.

- Puntuar agentes facilitadores:

Antes de describir los pasos a seguir, es importante señalar que el proceso de puntuación deber realizarse para cada uno de los conceptos siguientes: sólidamente fundamentado, integrado, implantado, sistemático, medición, aprendizaje y mejora. Son los conceptos en los que el modelo divide el enfoque, despliegue, evaluación y revisión. Al final de las puntuaciones individuales, se

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

dará una puntuación global para el enfoque, otra para el despliegue y una adicional para la evaluación y revisión. Es importante señalar que las puntuaciones en EFQM se suelen realizar con múltiplos de 5. “Afinar más” no suele aportar ningún matiz relevante a los objetivos que se pretenden conseguir.

1- Revisar los puntos fuertes y áreas de mejora identificados para el subcriterio analizado.

2- En primer lugar, elegir la caja de la matriz que contenga el concepto que mejor describa la relación entre puntos fuertes y áreas de mejora que se han detectado. Se dispone de 5 posibilidades, desde “sin evidencia” hasta “evidencia total”, (aunque también aparece desde “implantado en ¼ de las áreas” hasta “implantado en todas las áreas”).

3- Una vez seleccionada la caja adecuada, situarse en el valor central de la misma. En este momento decidir si a tenor de los puntos fuertes y áreas de mejora disponibles se debe elegir el valor central o corregirlo hacia arriba o hacia abajo. Esa será la puntuación definitiva obtenida.

4- Una vez obtenida la puntuación individual de los conceptos que componen, el enfoque, el despliegue y la evaluación y revisión, se deberá decidir la puntuación global de cada uno de estos tres. Recordar que no es una cuestión necesariamente de medias. Sobre todo, si se tiene puntuaciones muy dispares entre sí. Por ejemplo, puede darse el caso de que “implantado” esté puntuado con un 65 y “sistemático” con un 15. Una puntuación media de 40 no sería del todo correcta para puntuar el despliegue, debiendo darle cierta importancia al hecho de presentarse una puntuación tan baja como lo es el 15. Tal vez en este caso una puntuación de 30 ó 35 podría ser adecuada. En cualquier caso, valorar siempre la situación concreta que se está puntuando.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

5- Decidir la puntuación total. Esta se obtendrá valorando las puntuaciones obtenidas en el enfoque, despliegue y en la evaluación y revisión.

- Puntuar resultados:

La sistemática es la misma. El proceso de puntuación ahora debe centrarse en analizar los indicadores disponibles en relación a: sus tendencias, objetivos, comparaciones, causas y ámbito de aplicación. Es importante recordar que cuando se evalúan resultados (indicadores) no se está valorando las actividades que los provocan. Se está evaluando simple y llanamente un número y unas características muy concretas de ese número.

#### Realizar reuniones de consenso

Al finalizar las evaluaciones individuales se realizará una reunión de consenso en la que se debatirán los puntos fuertes, áreas de mejora y puntuación, entre el equipo de autoevaluación. La gran ventaja al realizar esta reunión es que el equipo descubrirá que cada miembro aportará matices y reflexiones diferentes que enriquecerán el análisis final obtenido. Durante la misma, se deberá tener presente que el objetivo es precisamente buscar consenso en relación a los análisis individuales. Para ello se recomienda:

- Leer todas las áreas de mejora y puntos fuertes, de criterios tanto facilitadores como de resultados.

- Permitir que todos los agentes aporten sus puntos fuertes y áreas de mejora detectadas. No descartar ninguno antes de analizarlo por insignificante que parezca.

Por otro lado, siempre se deberá tener en cuenta que:

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Víctor E. Vera Pinto

- Puntuar con EFQM no es una ciencia exacta.
- La percepción que las personas tienen de la excelencia difiere.
- La comprensión que las personas tienen de los criterios y de la hoja REDER es diferente.

### Resumen final de puntuaciones

El cálculo de las puntuaciones se llevará a cabo teniendo en cuenta que la puntuación máxima que se puede obtener en el Modelo Europeo de Excelencia es de 1000 puntos, distribuidos de la siguiente forma:

1. Liderazgo (100 puntos).
2. Política y estrategia (80 puntos).
3. Desarrollo de las personas (90 puntos).
4. Recursos y asociados (90 puntos).
5. Clientes (140 puntos).
6. Resultados en los clientes (200 puntos).
7. Resultados en las personas (90 puntos).
8. Resultados en sociedad (60 puntos).
9. Resultados clave (110 puntos).

A continuación, se muestra la forma cómo deben ser calculadas las puntuaciones finales de cada criterio:

Criterios facilitadores:

Criterio número	1	%	2	%	3	%	4	%	5	%
Subcriterio	1a		2a		3a		4a		5a	

Subcriterio	1b		2b		3b		4b		5b	
Subcriterio	1c		2c		3c		4c		5c	
Subcriterio	1d		2d		3d		4d		5d	
Subcriterio	1e				3e		4e		5e	
Total		÷5		÷4		÷5		÷5		÷5
Puntuación										

Tabla 11. Metodología de cálculo de puntuaciones para criterios facilitadores. Fuente: Moreno (2007).

Anotar las puntuaciones de cada subcriterio.  
 Sumar y dividir por el número de subcriterios.  
 Esa será la puntuación definitiva para un criterio.

Criterios resultados:

Criterio número	6	%			7	%			8	%			9	%		
Subcriterio	6a		X 0,75		7a		X 0,75		8a		X 0,75		9a		X 0,75	
Subcriterio	6b		X 0,25		7b		X 0,25		8b		X 0,25		9b		X 0,25	
Puntuación																

Tabla 12. Metodología de cálculo de puntuaciones para criterios resultados. Fuente: Moreno (2007).

Anotar las puntuaciones de cada subcriterio.  
 Multiplicar por su peso porcentual y sumar.  
 Esa será la puntuación definitiva para un criterio.

Cálculo de la puntuación total:

Criterio	Puntuación %	Factor	Puntos
1.- Liderazgo		X 0,1	
2.- Política y estrategia		X 0,8	
3.- Gestión del personal		X 0,9	
4.- Recursos		X 0,9	
5.- Procesos		X 1,4	
6.- Resultados del cliente		X 2,0	
7.- Resultados del personal		X 0,9	
8.- Resultados en la sociedad		X 0,6	
9.- Resultados claves		X 1,5	
Total puntos			

Tabla 13. Cálculo de puntuación total. Fuente: Moreno (2007).

Anotar la valoración asignada a cada criterio.  
 Multiplicar cada valoración por su factor para obtener los puntos parciales.  
 Sumar los puntos parciales de cada criterio para obtener la puntuación final.

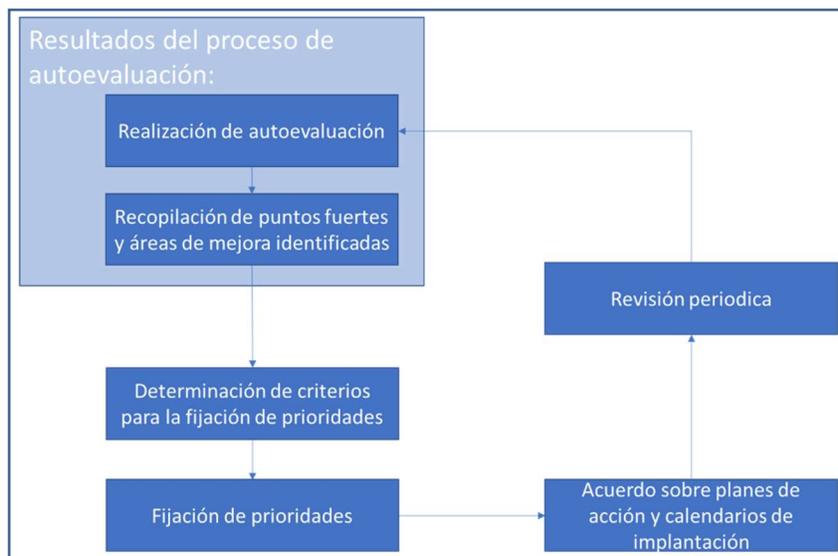
### **Proceso de planes de acción para la mejora**

Una vez finalizadas todas las reuniones de consenso, se desarrollara un informe en el que se recopilen todas las conclusiones definitivas, en el que se incluyan los puntos fuertes, áreas de mejora y puntuación para cada uno de los subcriterios.

La autoevaluación permitirá a la organización identificar un número importante de acciones de mejora. Sin embargo, no hay que perder de vista que el objetivo de la autoevaluación no termina ahí. El objetivo es descubrir mejoras, pero no llevarlas a la práctica dejara a la organización en el mismo sitio en el que se está.

Esta situación, es la que provoca que muchas organizaciones abandonen la utilización del modelo de excelencia. Las expectativas planteadas en un principio se ven truncadas ante la imposibilidad de realizar las mejoras identificadas. Tal vez, uno de los problemas de las organizaciones para implantar las mejoras sea la metodología empleada para este fin. Para evitar esto se deberá presentar una metodología lógica y simple, que puede facilitar el camino y a su vez nunca puede suplir a la verdadera fuerza impulsora de la implicación de la dirección.

El gráfico siguiente resume el proceso a seguir para implantar las mejoras identificadas:



**Ilustración 11. Resumen de proceso de planes de acción. Fuente: Elaboración propia.**

Una vez realizada la autoevaluación y recopilados los puntos fuertes y áreas de mejora, el primer paso a realizar consistirá en la determinación de los criterios para priorizar ésta últimas.

Para seleccionar los criterios de priorización pueden tenerse en cuenta los siguientes conceptos:

- FCE (Factor crítico de éxito) relevantes para la organización.
- Objetivos estratégicos.
- Resultados clave.
- Requisitos de clientes, personas o sociedad.

Seguidamente, una vez definidos los criterios a utilizar, se elegirán las áreas de mejora que más impacten en los criterios utilizados. Para identificarlas, es conveniente realizar una tabla que cruce las mejoras con los diferentes criterios. Con esta tabla se puede obtener una puntuación que

puede ayudar a decidir qué mejoras realizar. Es importante resaltar que la selección de las áreas de mejora se puede realizar mediante la utilización de los mencionados “ejes transversales”.

Acción	Impacto sobre la organización	Capacidad para implantarla	Puntuación	Rankin

**Tabla 14. Modelo de tabla de puntuación de acciones de mejora. Fuente: Elaboración propia.**

Ya elegidas las mejoras prioritarias, el siguiente paso consistirá en hacer un calendario de implantación de las mismas. En este momento, es imprescindible asignar un propietario o responsable de la ejecución de cada una de las acciones. Así mismo, es importante establecer la fecha prevista de finalización de la misma.

Prioridad en el ranking	Acción	Propietario	Fecha Finalizac.	Diagrama Gantt de acciones									Estado
				1	2	3	4	5	6	7	8	9	

**Tabla 15. Modelo de calendario de implantación de acciones de mejora. Fuente: Elaboración propia.**

El siguiente paso consistirá en la ejecución de la acción de mejora. Es muy recomendable, que la propia acción de mejora siga la sistemática vista hasta ahora, debiendo definir cómo se realiza el:

- Enfoque y/o planificación de la acción.
- Despliegue o implantación de la acción.
- Medición de resultados de la acción.

- Evaluación y revisión de la acción.

Definición de acción de mejora	
Propietario	Fecha de finalización
Prioridad del ranking	Criterio del modelo
Estado actual	<input type="checkbox"/> Rojo <input type="checkbox"/> Ámbar <input type="checkbox"/> Verde
Enfoque: Descripción de la acción de mejora y de las razones de su selección	
Despliegue: ¿Cómo se despliega el enfoque?	
Resultados: ¿Qué resultados se obtienen en su despliegue (plazos, alcance, etc)?	Comentarios
Evaluación y revisión: ¿Cómo y cuándo se está evaluando?	Comentarios

Tabla 16. Modelo de tabla para control de ejecución de acciones de mejora. Fuente: Elaboración propia,

Por último, todas las acciones de mejora serán tenidas en cuenta para el desarrollo de la siguiente autoevaluación. En ésta se verificará la implantación de las mismas y se detectarán nuevas acciones que vuelvan a poner en marcha el proceso descrito en este capítulo.

## **4.5 Recomendaciones**

Finalmente, luego de presentadas las bases de una propuesta de modelo parcial de excelencia EFQM para la ciberseguridad en España, resulta relevante hacer mención de hallazgos que se hicieron presentes durante esta investigación. Los cuales, a pesar de no estar directamente asociado a la implementación del modelo, su consideración sin duda podrá facilitar su implantación y exitoso desarrollo. Estos hallazgos son:

- El contexto internacional actual de ciberamenazas, exige a los países el asumir el potenciar los procesos I+D+i de ciberseguridad como una prioridad.

- La inconclusa postura reflejada en la ECN en materia de actividades I+D+i es una carencia que incide sobre la designación de un referente en el sector. Las acciones llevadas a cabo por el INCIBE resuelven este vacío, pero aún hay camino por recorrer para involucrar a más agentes a las actividades de la Red.

- La metodología de trabajo de la Comisión Europea no incluye un plan específico en I+D+i, demostrando que al ser sustituido por un programa de trabajo definido por todos sus miembros se logran proyectos con mayor alcance y diversidad, tanto en las tecnologías consideradas como en redes que involucra.

- El modelo EFQM desde su implantación requiere de una mayor participación posible de los miembros de la organización en la que se aspira sea implantado, por lo que el modelo propuesto solo deberá ser considerado por el Comité de Calidad como una propuesta. Será su obligación llegar a un mayor detalle sobre las necesidades y oportunidades presentes en sus facilitadores.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en*

*España dentro de un marco I+D+i*

Victor E. Vera Pinto

- El modelo EFQM de excelencia es una marca registrada, por lo que se invita al RENIC a previo a la evaluación de su implantación, contactar a [www.efqm.org/](http://www.efqm.org/).

## ANEXOS

### Anexo I. Resumen de investigaciones consultadas de menor aportación.

Autor	Año	Título	Área de Aportación
Calvo-Mora et al.	2016	“Prácticas de gestión de excelencia, gestión del conocimiento y resultados empresariales en las grandes organizaciones y las pymes: Un análisis multi-grupal”	Modelo de excelencia EFQM / I+D+i / Gobernanza.
Jaeger & Matyas	2016	“Transformación del enfoque EFQM del negocio hacia la excelencia en las operaciones”	Modelo de excelencia EFQM.
Gómez-Gómez et al.	2016	“Ponderación de las dimensiones en los modelos de excelencia - una revisión crítica desde una perspectiva empresarial”	Modelo de excelencia EFQM / Gobernanza.
Zubizarreta et al.	2016	“ <i>Innovation evaluation model for macro-construction sector companies: A study in Spain</i> ”	I+D+I /Gobernanza.
UK Cabinet office	2016	“ <i>The UK cyber security strategy 2011-2016: annual report</i> ”	Ciberseguridad / I+D+I / Gobernanza / TIC
Cendoya	2016	“ <i>National cyber security organization: Spain</i> ”	Ciberseguridad / Gobernanza
Comisión Europea	2016	“ <i>Digital economy and society index</i> ”	TIC / Ciberseguridad / Gobernanza
Fischer	2016	“ <i>Cybersecurity issues and challenges: in brief</i> ”	TIC / Ciberseguridad / Gobernanza
INCIBE	2016	“Tendencias en el mercado de la ciberseguridad”	TIC / Ciberseguridad / Gobernanza
ONTSI	2016	“Informe de ONTSI”	TIC / Ciberseguridad / Gobernanza / I+D+i
Polo tecnológico de ciberseguridad en España	2016	“Informe de internacionalización de empresas”	Ciberseguridad / Gobernanza / I+D+i
Skopik et al.	2016	“ <i>A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing</i> ”	Ciberseguridad / Gobernanza / I+D+i

<b>Smith et al.</b>	2016	<i>“Going beyond cybersecurity compliance: what power and utility companies really need to consider”</i>	Ciberseguridad / Gobernanza
<b>Weber et al.</b>	2016	<i>“Cyber security in the internet of things: Legal aspects”</i>	Ciberseguridad / Seguridad de la información / Gobernanza
<b>Addae et al.</b>	2016	<i>“An augmented cybersecurity behavioral research model”</i>	Ciberseguridad / I+D+i / Gobernanza
<b>Elliott et al.</b>	2016	<i>“Action, inaction, trust, and cybersecurity's common property problem”</i>	Ciberseguridad / Gobernanza / I+D+i
<b>Burdon et al.</b>	2016	<i>“The regulatory challenges of Australian information security practice”</i>	Ciberseguridad / Seguridad de la información / Gobernanza
<b>Jorgenson &amp; Vu</b>	2016	<i>“The ICT revolution, world economic growth, and policy issues”</i>	TIC / Ciberseguridad / Gobernanza / I+D+i
<b>Fisher</b>	2016	<i>“Addressing pressing cybersecurity issues through collaboration”</i>	Ciberseguridad / Gobernanza / I+D+i
<b>Antonescu &amp; Birau</b>	2015	<i>“Financial and non-financial implications of cybercrimes in emerging countries”</i>	Ciberseguridad / Gobernanza
<b>Fazlida &amp; Said</b>	2015	<i>“Information Security: Risk, Governance and Implementation Setback”</i>	Ciberseguridad / Gobernanza
<b>Korff</b>	2015	<i>“Selection of cyber security definitions”</i>	Ciberseguridad / Seguridad de la información
<b>Leiva</b>	2015	<i>“Estrategias nacionales de ciberseguridad: Estudio comparativo basado en enfoque top-down desde una visión global a una visión local”</i>	Ciberseguridad / Gobernanza
<b>Department of defense, US</b>	2015	<i>“The DoD cyber strategy”</i>	Ciberseguridad / Seguridad de la información / Gobernanza / TIC
<b>Araújo y Sampaio</b>	2014	<i>“El camino hacia la excelencia de las organizaciones portuguesas reconocidas por el modelo EFQM”</i>	Modelo de excelencia EFQM

<b>Onyeji et al.</b>	2014	“ <i>Cyber Security and Critical Energy Infrastructure</i> ”	Ciberseguridad / Gobernanza
<b>Comisión Europea</b>	2014	“ <i>Digital Agenda for Europe – Netherlands</i> ”	TIC / Ciberseguridad / Gobernanza
<b>Comisión Europea</b>	2014	“ <i>Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace</i> ”	TIC / Ciberseguridad / Gobernanza / I+D+i
<b>Harkins</b>	2013	“ <i>Managing Risk and Information Security</i> ”	Ciberseguridad / Seguridad de la información / Gobernanza
<b>Presidencia del Gobierno de España</b>	2013	“Estrategia de Ciberseguridad Nacional”	Ciberseguridad / Gobernanza
<b>Chardentaseva et al.</b>	2013	“ <i>A Reference Model of Information Assurance &amp; Security</i> ”	Ciberseguridad / Seguridad de la información / Gobernanza
<b>Du et al.</b>	2012	“Aplicación del modelo de excelencia basado en EFQM en proyectos PPP”	Modelo de excelencia EFQM
<b>Chamorro et al.</b>	2012	“La Ciberseguridad nacional, un compromiso de todos. La necesidad de evolucionar de una cultura reactiva a una de prevención y resiliencia”	Ciberseguridad / Seguridad de la información / Gobernanza
	2012	“ <i>Some Perspectives on Cybersecurity: 2012</i> ”	TIC / Ciberseguridad / Gobernanza
<b>Whitman &amp; Mattord</b>	2012	“ <i>Principles of information security</i> ”	Ciberseguridad / Seguridad de la información / Gobernanza
<b>UK Cabinet office</b>	2011	“ <i>The UK Cyber Security Strategy Protecting and promoting the UK in a digital world</i> ”	Ciberseguridad / Seguridad de la información / Gobernanza / I+D+i / TIC
<b>De Leeuw</b>	2009	“ <i>The history of information security: A comprehensive handbook</i> ”	Ciberseguridad / Seguridad de la información
<b>Morera &amp; Mascarell</b>	2009	“Caminos para la innovación en la empresa: el modelo de Kline”	I+D+i / Gobernanza

<b>International telecommunication union</b>	2008	<i>“Data networks, open system communications and security Public: Overview of cybersecurity”</i>	Ciberseguridad / Seguridad de la información
<b>Pujol &amp; Vivó</b>	2008	<i>“I+D+i: Una perspectiva documental”</i>	I+D+i / Gobernanza
<b>International telecommunication union</b>	2008	<i>“The ITU National Cybersecurity Strategy Guide”</i>	Ciberseguridad / Seguridad de la información / Gobernanza
<b>Stamp</b>	2005	<i>“Information security principles and practice”</i>	Ciberseguridad / Seguridad de la información /
<b>Venter &amp; Eloff</b>	2004	<i>“Vulnerability Forecasting-a Conceptual Model”</i>	Ciberseguridad
<b>Anderson</b>	2003	<i>“Why we need a new definition of information security”</i>	Ciberseguridad / Seguridad de la Información
<b>Blakley et al.</b>	2001	<i>“Information security is information risk management”</i>	Seguridad de la información
<b>Pipkin</b>	2000	<i>“Information Security: Protecting the Global Enterprise”</i>	Seguridad de la información
<b>McCumber</b>	1991	<i>“Information System Security: A Comprehensive Model”</i>	Seguridad de la información

Tabla 17. Relación de antecedentes de la investigación revisados.

**Anexo II. Quick self-assessment propuesto por EFQM (2012) para diagnosticar la necesidad de la implantación del modelo EFQM para agencias de innovación.**

	<b>Fundamental Concept</b>	<b>Approach</b>	<b>Guidance</b>
1	<i>Sustaining outstanding results</i>	<i>Business Planning Process</i>	<i>The approach you use for prioritizing and planning your future activities, in line with your stakeholder needs and expectations.</i>
2	<i>Sustaining outstanding results</i>	<i>Target Setting Process</i>	<i>The approach you use for setting performance targets for your key performance indicators, both financial and non-financial, in line with stakeholder expectations.</i>
3	<i>Sustaining outstanding results</i>	<i>Balanced Scorecard or Top Level Management Report</i>	<i>The approach you use to develop the framework of measures you use to track performance against strategic objectives, usually for review by the management team.</i>
4	<i>Adding Value to Customers</i>	<i>Customer Relationship Management</i>	<i>The approach you have developed for understanding and meeting the needs and expectations of your customers.</i>
5	<i>Adding Value to Customers</i>	<i>Complaints Management Process</i>	<i>The approach you use for ensure customer complaints are captured and resolved effectively and efficiently.</i>
6	<i>Adding Value to Customers</i>	<i>Customer Survey</i>	<i>The approach you have for collecting structured customer perception data to enable the review of "customer relationship management".</i>
7	<i>Developing Organizational Capability</i>	<i>Benchmarking Strategy</i>	<i>The approach you have for comparing the effectiveness and efficiency of your key processes and approaches against suitable external benchmarks.</i>
8	<i>Developing Organizational Capability</i>	<i>Partnership Policy &amp; Guidelines</i>	<i>The approach you use for identifying, forming and developing relationships with external partners whose core products and services compliment those of your organization.</i>
9	<i>Developing Organizational Capability</i>	<i>Creating and benefiting from a network</i>	<i>The approach you use to build a network that supports and contributes to your organization's objectives</i>
10	<i>Managing with Agility</i>	<i>Process Framework Defined &amp; Mapped</i>	<i>The approach you use for defining and documenting the framework of key processes required to effectively implement your strategy.</i>
11	<i>Managing with Agility</i>	<i>Process Ownership Defined</i>	<i>The approach you use for defining ownership and responsibility for managing your key processes.</i>
12	<i>Managing with Agility</i>	<i>Process Improvement Methodology</i>	<i>The approach used for identifying, prioritizing and implementing process improvements, including ensuring they have had the desired impact on improving the effectiveness and efficiency.</i>
13	<i>Leading with Vision, Inspiration and Integrity</i>	<i>Clear Vision, Mission &amp; Values statements</i>	<i>The approach you have for defining and refining the organization's Vision, Mission and Values.</i>
14	<i>Leading with Vision, Inspiration and Integrity</i>	<i>KPI Report &amp; Review Meeting</i>	<i>The approach you use to regularly review performance against your key objectives and agree appropriate improvement actions and tactical responses to performance levels achieved.</i>

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en*

*España dentro de un marco I+D+i*

Victor E. Vera Pinto

15	<i>Succeeding through the Talent of People</i>	<i>Employee Appraisal Process</i>	<i>The approach you use for setting individual or team objectives and reviewing and improving personal performance.</i>
16	<i>Succeeding through the Talent of People</i>	<i>Employee Survey</i>	<i>The approach you have for collecting structured people perception data to enable the review of HR policies and processes.</i>
17	<i>Harnessing Creativity &amp; Innovation</i>	<i>Market Research &amp; Analysis</i>	<i>The approach you use for understanding changes and performance levels within the external environment your organization operates in.</i>
18	<i>Harnessing Creativity &amp; Innovation</i>	<i>Knowledge Management Strategy</i>	<i>The approach you use for ensuring people, both within and outside your organization, have access to accurate, reliable and timely information that will enable the effective execution of your key processes and the achievement of your strategic objectives.</i>
19	<i>Taking Responsibility for a Sustainable Future</i>	<i>Environmental Management Policy</i>	<i>The approach you have to determining, managing and minimizing the impact of your operations on the environment.</i>
20	<i>Taking Responsibility for a Sustainable Future</i>	<i>CSR Policy</i>	<i>The approach you have adopted to understanding and maximizing your contribution to society, whether locally or globally.</i>

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

**Anexo III. Correo electrónico de invitación a participar en cuestionario.**

Correo :: Estudio del ecosistema de ciberseguridad en España dentro del marco I+D+i - Cuestionario a agentes relevantes, ...

Universitat Politècnica de València [ES] | <https://webmail.upv.es/imp/dynamic.php?page=message&buid=65&mailbox=SU5>

← Responder → Reenviar Eliminar

**Estudio del ecosistema de ciberseguridad en España dentro del marco I+D+i - Cuestionario a agentes relevantes.** Ver origen Guardar

Fecha: 28/02/17 (20:59:21 CEST)  
De: Victor Vera  
Para: contacto@renic.es  
Bcc: escmarlu@jcy.l.es | gardieja@jcy.l.es | martin.muehleck@ec.europa.eu | jdavila@fi.upm.es | peter.bryant@ie.edu | jlhardieta@indra.es | secretario-tecnico@pesi-seguridadindustrial.org | jestevez@inf.uc3m.es | pgteodor@ugr.es | santos@uniovi.es | fperez@gts.uvigo.es | troncoso@gts.uvigo.es | villagra@dit.upm.es | jose.narbona@uah.es | maite.boyero@cdti.es | gerente@conetic.info | rafael.ortega@i4s.com | jorge.lopez\_vergara@uam.es | francisco.ruiz@uclm.esg | javiergv@fdi.ucm.es | juanramon.velasco@uah.es | zamora@dccia.ua.es | pmacia@dtic.ua.es | pcaballe@ull.edu.es | jlm@lcc.uma.es | ruribeetxeberria@mondragon.edu | gregorio@um.es | gasca@us.es | begona.blanco@ehu.eus | eduardo.jacob@ehu.es | joseluis.martin@ehu.eus | agomez@diatel.upm.es | berrocal@dit.upm.es | eduardo.magana@unavarra.es | jaume.pujol@uab.cat | dmegias@uoc.edu | Javier.herranz@upc.edu | jorge@ac.upc.es | soriano@entel.upc.es | calafate@disca.upv.es | josep.domingo@urv.cat | mjuan@s2grupo.es

Estimado:  
Empresario / Académico / Investigador (a).

Reciba un cordial saludo.

Mi nombre es Víctor Vera Pinto y soy estudiante del Máster en Gestión de Empresas Productos y Servicios de la Universidad Politècnica de Valencia.  
Se está realizando un estudio con agentes pertenecientes al ecosistema de ciberseguridad en España para determinar la necesidad de implementar en la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), un modelo parcial de excelencia EFQM para la definición de las estrategias a seguir para alcanzar sus objetivos orientados a la excelencia.

Esta encuesta está dirigida hacia los agentes relevantes del ecosistema de ciberseguridad en España dentro del marco I+D+i, establecidos así por el INCIBE en su "Estudio de viabilidad, oportunidad y diseño de una red de centros de excelencia en I+D+i en ciberseguridad". Por esta razón, se le invita a participar en el cuestionario titulado: "Cuestionario orientado a determinar la necesidad de un modelo parcial de excelencia EFQM para desarrollo del ecosistema de ciberseguridad en España dentro del marco I+D+i"

La recolección de datos se realizara en el periodo comprendido entre el 01/03/2017 y el 14/03/2017 y el tiempo estimado para realizar este cuestionario es de 10 minutos. Sus respuestas serán tratadas de manera anónima y con una finalidad totalmente científica. Tenga en cuenta además, que al finalizar este estudio se les hará llegar un correo electrónico con un resumen descriptivo. En este resumen, su nombre solo aparecerá en el apartado de agradecimientos.

Por favor siga el siguiente enlace para realizar la cuestionario descrito:

[https://docs.google.com/forms/d/e/1FAIpQLSc9m4Ch7GQPxBWxH19s8\\_uEyLF0fff8EKm69hHUt3\\_pzo8lQ/viewform](https://docs.google.com/forms/d/e/1FAIpQLSc9m4Ch7GQPxBWxH19s8_uEyLF0fff8EKm69hHUt3_pzo8lQ/viewform)

Agradeciendo de antemano su disposición y colaboración para el estudio.  
Un saludo,  
Víctor E. Vera Pinto.

## **Anexo IV. Cuestionario orientado a determinar la necesidad de un modelo parcial de excelencia EFQM para el desarrollo del ecosistema de ciberseguridad en España dentro del marco I+D+i.**

Este cuestionario busca determinar el grado de madurez en el que se encuentran las estrategias asumidas por el RENIC para alcanzar los siguientes objetivos estratégicos:

- Fomento de la excelencia de los equipos de investigación avanzada en ciberseguridad nacional potenciando sus capacidades y aumentando el grado de colaboración y conexión entre sus agentes.
- Mejorar la conexión del sector académico-investigador con la industria de ciberseguridad potenciando la transferencia de tecnología y conocimiento.
- Fomentar la difusión y promoción de los resultados de la I+D+i de excelencia.
- Identificar, atraer, generar, retener y desarrollar profesionales en ciberseguridad a nivel nacional.
- Actuar como facilitador para encontrar fórmulas de financiación para que los agentes del ecosistema puedan financiar sus proyectos de I+D+i en ciberseguridad.

Siendo usted un agente representativo en el ecosistema de ciberseguridad en el marco de I+D+i, indique el grado de madurez de los objetivos estratégicos antes enunciados del RENIC. Para esto se le presentan 20 enfoques de líneas de acción con cinco opciones para juzgar el nivel de desarrollo (desde "Nada desarrollada" hasta "Madura con mejoras continuas") en el que se encuentra actualmente cada uno de los enfoques que se describen a continuación:

1. La estrategia utilizada por el RENIC para el establecimiento de prioridades y la planificación de actividades futuras alineadas con las necesidades y expectativas de los agentes del ecosistema.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_
- d) Madura con mejoras por realizar. \_\_\_
- e) Madura con mejoras continuas. \_\_\_

2. La estrategia que utilizada por el RENIC para establecer objetivos de rendimiento para sus indicadores de desempeño clave, tanto en el ámbito financiero como en el no financieros, de acuerdo con las expectativas de los agentes involucrados en la red.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

3. La estrategia utilizada por el RENIC para desarrollar el marco de referencia de las medidas a utilizar para realizar un seguimiento del desempeño en relación con los objetivos estratégicos.

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

4. La estrategia utilizada por el RENIC para comprender y satisfacer las necesidades y expectativas de sus clientes.

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

5. La estrategia utilizada por el RENIC para garantizar que las quejas de los clientes son detectadas y resueltas de manera eficaz y eficiente.

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

6. La estrategia utilizada por el RENIC para recopilar datos estructurados de la percepción de sus clientes, buscando realizar la revisión continua del "*customer relationship management*".

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

7. La estrategia utilizada por el RENIC para comparar la eficacia y la eficiencia de sus procesos y objetivos clave con los benchmarks externos adecuados.

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

8. La estrategia utilizada por el RENIC para identificar, formar y desarrollar relaciones con socios externos cuyos productos y servicios complementan a los de los agentes pertenecientes a la Red.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_
- d) Madura con mejoras por realizar. \_\_\_
- e) Madura con mejoras continuas. \_\_\_

9. La estrategia utilizada por el RENIC para construir una red que soporte y contribuye a los objetivos de su organización.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_
- d) Madura con mejoras por realizar. \_\_\_
- e) Madura con mejoras continuas. \_\_\_

10. La estrategia utilizada por el RENIC para definir y documentar el marco de los procesos clave necesarios para implementar eficazmente su estrategia.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_
- d) Madura con mejoras por realizar. \_\_\_
- e) Madura con mejoras continuas. \_\_\_

11. La estrategia utilizada por el RENIC para definir la propiedad y la responsabilidad de administrar sus procesos clave.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_
- d) Madura con mejoras por realizar. \_\_\_
- e) Madura con mejoras continuas. \_\_\_

12. La estrategia utilizada por el RENIC para identificar, priorizar e implementar mejoras de procesos, incluyendo asegurar que han tenido el impacto deseado en la mejora de la eficacia y eficiencia.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_
- d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

13. La estrategia utilizada por el RENIC para definir y perfeccionar su Visión, Misión y Valores.

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

14. La estrategia utilizada por el RENIC para revisar periódicamente el desempeño en relación con sus objetivos claves y acordar las acciones de mejora apropiadas y las respuestas tácticas a los niveles de desempeño alcanzados.

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

15. La estrategia utilizada por el RENIC para establecer proyectos individuales o de grupo (constructo-nodal) y revisar y mejorar el rendimiento individual.

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

16. La estrategia utilizada por el RENIC para recopilar datos estructurados de percepción las personas involucradas de forma activa a la red buscando la revisión continua de políticas y procesos de recursos humanos.

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

17. La estrategia utilizada por el RENIC para comprender los cambios y los niveles de rendimiento en el entorno internacional en el que opera.

a) Nada desarrollada. \_\_\_

b) En sus primeros pasos de madurez. \_\_\_

c) Madura sin mejoras previstas. \_\_\_

d) Madura con mejoras por realizar. \_\_\_

e) Madura con mejoras continuas. \_\_\_

18. La estrategia utilizada por el RENIC para garantizar que las personas, tanto dentro como fuera de su organización, tengan acceso a información precisa, confiable y oportuna que permita la ejecución efectiva de sus procesos clave y el logro de sus objetivos estratégicos.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_
- d) Madura con mejoras por realizar. \_\_\_
- e) Madura con mejoras continuas. \_\_\_

19. La estrategia utilizada por el RENIC para determinar, gestionar y minimizar el impacto de sus operaciones en el medio ambiente.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_
- d) Madura con mejoras por realizar. \_\_\_
- e) Madura con mejoras continuas. \_\_\_

20. La estrategia utilizada por el RENIC para comprender y maximizar su contribución a la sociedad, ya sea localmente o internacionalmente.

- a) Nada desarrollada. \_\_\_
- b) En sus primeros pasos de madurez. \_\_\_
- c) Madura sin mejoras previstas. \_\_\_
- d) Madura con mejoras por realizar. \_\_\_
- e) Madura con mejoras continuas. \_\_\_

**Anexo V. Resultados obtenidos de Cuestionario orientado a determinar la necesidad de un modelo parcial de excelencia EFQM para el desarrollo del ecosistema de ciberseguridad en España dentro del marco I+D+i.**

Concepto fundamental de excelencia considerado: *Sustaining outstanding results.*

Las organizaciones excelentes alcanzarán mantener resultados excepcionales que permitan cubrir las necesidades a corto y largo plazo de los agentes, dentro del contexto operacional en el que se desenvuelven.

Resultados obtenidos:

Enfoque considerado	Línea de acción propuesta en cuestionario	Respuestas obtenidas de aplicación de cuestionario
Business Planning Process	1. La estrategia utilizada por el RENIC para el establecimiento de prioridades y la planificación de actividades futuras alineadas con las necesidades y expectativas de los agentes del ecosistema.	<ul style="list-style-type: none"> <li>Nada desarrollada</li> <li>En sus primeros pasos de madurez</li> <li>Madura sin mejoras previstas</li> <li>Madura con mejoras por realizar</li> <li>Madura con mejoras continuas</li> </ul>
Target Setting Process	2. La estrategia que utilizada por el RENIC para establecer objetivos de rendimiento para sus indicadores de desempeño clave, tanto en el ámbito financiero como en el no financieros, de acuerdo con las expectativas de los agentes involucrados en la red.	<ul style="list-style-type: none"> <li>Nada desarrollada</li> <li>En sus primeros pasos de madurez</li> <li>Madura sin mejoras previstas</li> <li>Madura con mejoras por realizar</li> <li>Madura con mejoras continuas</li> </ul>
Balanced Scorecard or Top Level Management Report	3. La estrategia utilizada por el RENIC para desarrollar el marco de referencia de las medidas a utilizar para realizar un seguimiento del desempeño en relación con los objetivos estratégicos	<ul style="list-style-type: none"> <li>Nada desarrollada</li> <li>En sus primeros pasos de madurez</li> <li>Madura sin mejoras previstas</li> <li>Madura con mejoras por realizar</li> <li>Madura con mejoras continuas</li> </ul>

Tabla 18. Resultados de cuestionario - *Sustaining outstanding results.* Fuente Elaboración propia

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

Concepto fundamental de excelencia considerado: *Adding value for customers*.

Las organizaciones excelentes constantemente buscaran adherir valor entendiendo, anticipando y cubriendo las necesidades, expectativas y oportunidades desde la perspectiva del consumidor.

Resultados obtenidos:

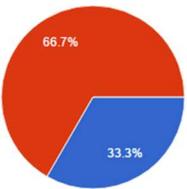
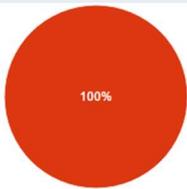
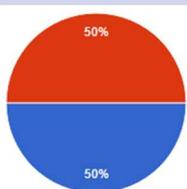
Enfoque considerado	Línea de acción propuesta en cuestionario	Respuestas obtenidas de aplicación de cuestionario
Customer Relationship Management	4. La estrategia utilizada por el RENIC para comprender y satisfacer las necesidades y expectativas de sus clientes.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>
Complaints Management Process	5. La estrategia utilizada por el RENIC para garantizar que las quejas de los clientes son detectadas y resueltas de manera eficaz y eficiente.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>
Customer Survey	6. La estrategia utilizada por el RENIC para recopilar datos estructurados de la percepción de sus clientes, buscando realizar la revisión continua del "customer relationship management".	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul> <p><b>Nota:</b> un participante se abstuvo de opinar sobre esta línea de acción.</p>

Tabla 19. Resultados de cuestionario - *Adding value for costumers*. Fuente Elaboración propia

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

Concepto fundamental de excelencia considerado: *Developing organizational capacity*:

Las organizaciones excelentes mejoraran su rendimiento mediante una efectiva gestión del cambio dentro y más allá de los límites de la organización.

Resultados obtenidos:

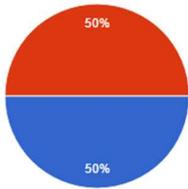
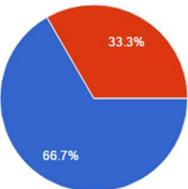
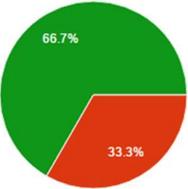
Enfoque considerado	Línea de acción propuesta en cuestionario	Respuestas obtenidas de aplicación de cuestionario
Benchmarking Strategy	7. La estrategia utilizada por el RENIC para comparar la eficacia y la eficiencia de sus procesos y objetivos clave con los benchmarks externos adecuados.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul> <p><i>Nota: un participante se abstuvo de opinar sobre esta línea de acción.</i></p>
Partnership Policy & Guidelines	8. La estrategia utilizada por el RENIC para identificar, formar y desarrollar relaciones con socios externos cuyos productos y servicios complementan a los de los agentes pertenecientes a la Red	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>
Creating and benefiting from a network	9. La estrategia utilizada por el RENIC para construir una red que soporte y contribuye a los objetivos de su organización.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>

Tabla 20. Resultados de cuestionario - *Developing organizational capacity*. Fuente Elaboración propia

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

Concepto fundamental de excelencia considerado: *Managing with agility*.

Las organizaciones excelentes serán ampliamente reconocidas por su habilidad de identificar y responder de manera eficiente y efectiva ante oportunidades como ante amenazas.

Resultados obtenidos:

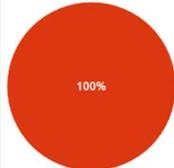
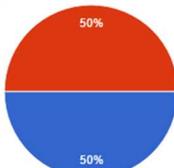
Enfoque considerado	Línea de acción propuesta en cuestionario	Respuestas obtenidas de aplicación de cuestionario
Process Framework Defined & Mapped	10. La estrategia utilizada por el RENIC para definir y documentar el marco de los procesos clave necesarios para implementar eficazmente su estrategia.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>
Process Ownership Defined	11. La estrategia utilizada por el RENIC para definir la propiedad y la responsabilidad de administrar sus procesos clave.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>
Process Improvement Methodology	12. La estrategia utilizada por el RENIC para identificar, priorizar e implementar mejoras de procesos, incluyendo asegurar que han tenido el impacto deseado en la mejora de la eficacia y eficiencia.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul> <p><b>Nota:</b> un participante se abstuvo de opinar sobre esta línea de acción.</p>

Tabla 21. Resultados de cuestionario - *Managing with agility*. Fuente Elaboración propia

Concepto fundamental de excelencia considerado: *Leading with vision, inspiration and integrity.*

Las organizaciones excelentes poseerán líderes que den forma al futuro haciéndolo posible, actuando como modelo a seguir por sus valores y sus planteamientos éticas.

Resultados obtenidos:

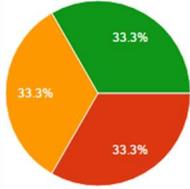
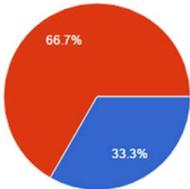
Enfoque considerado	Línea de acción propuesta en cuestionario	Respuestas obtenidas de aplicación de cuestionario
Clear Vision, Mission & Values statements	13. La estrategia utilizada por el RENIC para definir y perfeccionar su Visión, Misión y Valores	 <ul style="list-style-type: none"> <li><span style="color: blue;">●</span> Nada desarrollada</li> <li><span style="color: red;">●</span> En sus primeros pasos de madurez</li> <li><span style="color: orange;">●</span> Madura sin mejoras previstas</li> <li><span style="color: green;">●</span> Madura con mejoras por realizar</li> <li><span style="color: purple;">●</span> Madura con mejoras continuas</li> </ul>
KPI Report & Review Meeting	14. La estrategia utilizada por el RENIC para revisar periódicamente el desempeño en relación con sus objetivos claves y acordar las acciones de mejora apropiadas y las respuestas tácticas a los niveles de desempeño alcanzados.	 <ul style="list-style-type: none"> <li><span style="color: blue;">●</span> Nada desarrollada</li> <li><span style="color: red;">●</span> En sus primeros pasos de madurez</li> <li><span style="color: orange;">●</span> Madura sin mejoras previstas</li> <li><span style="color: green;">●</span> Madura con mejoras por realizar</li> <li><span style="color: purple;">●</span> Madura con mejoras continuas</li> </ul>

Tabla 22. Resultados de cuestionario - *Leading with vision, inspiration and integrity.* Fuente Elaboración propia

Concepto fundamental de excelencia considerado: *Succeeding through the talent of people*.

Las organizaciones excelentes valorarán a su gente y crearán una cultura de empoderamiento para la obtención de objetivos tanto organizacionales como personales.

Resultados obtenidos:

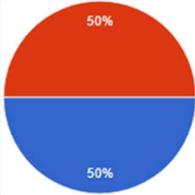
Enfoque considerado	Línea de acción propuesta en cuestionario	Respuestas obtenidas de aplicación de cuestionario
Employee Appraisal Process	15. La estrategia utilizada por el RENIC para establecer proyectos individuales o de grupo (constructo-nodal) y revisar y mejorar el rendimiento individual.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>
Employee Survey	16. La estrategia utilizada por el RENIC para recopilar datos estructurados de percepción las personas involucradas de forma activa a la red buscando la revisión continua de políticas y procesos de recursos humanos.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul> <p><b>Nota:</b> un participante se abstuvo de opinar sobre esta línea de acción.</p>

Tabla 23. Resultados de cuestionario - *Succeeding through the talent of people*. Fuente: Elaboración propia

Concepto fundamental de excelencia considerado: *Harnessing creativity and innovation*.

Las organizaciones excelentes generarán mayor valor y niveles de desempeño a través de mejoras continuas e innovaciones sistemáticas aprovechando la creatividad de sus agentes involucrados.

Resultados obtenidos:

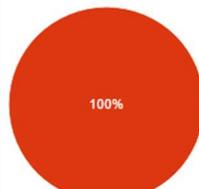
Enfoque considerado	Línea de acción propuesta en cuestionario	Respuestas obtenidas de aplicación de cuestionario
Market Research & Analysis	17. La estrategia utilizada por el RENIC para comprender los cambios y los niveles de rendimiento en el entorno internacional en el que opera.	 <p>100%</p> <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>
Knowledge Management Strategy	18. La estrategia utilizada por el RENIC para garantizar que las personas, tanto dentro como fuera de su organización, tengan acceso a información precisa, confiable y oportuna que permita la ejecución efectiva de sus procesos clave y el logro de sus objetivos estratégicos.	 <p>100%</p> <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>

Tabla 24. Resultados de cuestionario - *Harnessing creativity and innovation*. Fuente Elaboración propia

Concepto fundamental de excelencia considerado: *Creating a sustainable future*.

Las organizaciones excelentes tendrán un impacto positivo sobre el entorno en el que se desenvuelven mejorando su rendimiento y simultáneamente impulsando el avance económico, ambiental y social dentro de las comunidades a las cuales involucra.

Resultados obtenidos:

Enfoque considerado	Línea de acción propuesta en cuestionario	Respuestas obtenidas de aplicación de cuestionario
Environmental Management Policy	19. La estrategia utilizada por el RENIC para determinar, gestionar y minimizar el impacto de sus operaciones en el medio ambiente	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>
CSR Policy	20. La estrategia utilizada por el RENIC para comprender y maximizar su contribución a la sociedad, ya sea localmente o internacionalmente.	 <ul style="list-style-type: none"> <li>● Nada desarrollada</li> <li>● En sus primeros pasos de madurez</li> <li>● Madura sin mejoras previstas</li> <li>● Madura con mejoras por realizar</li> <li>● Madura con mejoras continuas</li> </ul>

Tabla 25. Resultados de cuestionario - *Creating a sustainable future*. Fuente Elaboración propia

**Importante:**

Durante un periodo de 11 días, el plazo establecido para la recolección de información a través del cuestionario fue suspendido a petición del presidente del RENIC (Ver anexo VII). Este evento pudo incidir en la cantidad de participantes en esta actividad.

## **Anexo VI. Protocolo de entrevista**

### **Apertura**

Buenas tardes, ¿Cómo te sientes?, ¿cómo te encuentras?, le informo que estoy haciendo mi trabajo final de master, en la Universidad Politécnica de Valencia. Yo soy estudiante y estoy realizando una investigación titulada: modelo parcial de excelencia EFQM para la ciberseguridad en España dentro del marco I+D+i.

Por lo cual le agradezco, que me responda con toda naturalidad, a su vez, necesito que me indique de qué tiempo dispone, y que me permita grabar la conversación, ya que no debo obviar ningún detalle en la investigación, usted permanecerá bajo el anonimato; si desea al transcribir la entrevista se la muestro para que compruebe que no se realizó ninguna modificación.

### **Desarrollo**

1. Establecer conocimientos comunes:

¿Conoce usted el RENIC?

- ¿Qué hace?
- ¿Quiénes conforman la RED?
- ¿Qué objetivos se plantea?
- ¿Reconoce usted la importancia del ecosistema de ciberseguridad en el marco de I+D+i en España?
- ¿Comprende la función que aspira desempeñar el RENIC en dicho ecosistema?

2. Capacidades y conocimientos del entrevistado en el área de estudio:

¿Conoce usted el modelo EFQM?

- Conoce los conceptos fundamentales de la excelencia
- Sistema de calidad en procesos de I+D+i.

Prácticas de I+D+i en ciberseguridad (Nacional/Internacional)

- ¿Certificaciones?
- Practicas actuales a nivel nacional
- Practicas actuales a nivel internacional

3. Análisis de necesidad del modelo por entrevistado

Oportunidades de mejora para el ecosistema de ciberseguridad en el marco I+D+i.

- *Sustaining outstanding results*

- La estrategia utilizada por el RENIC para el establecimiento de prioridades y la planificación de actividades futuras alineadas con las necesidades y expectativas de los agentes del ecosistema.
- La estrategia que utilizada por el RENIC para establecer objetivos de rendimiento para sus indicadores de desempeño clave, tanto en el ámbito financiero como en el no financieros, de acuerdo con las expectativas de los agentes involucrados en la red.
- La estrategia utilizada por el RENIC para desarrollar el marco de referencia de las medidas a utilizar para realizar un seguimiento del desempeño en relación con los objetivos estratégicos.
  
- *Adding value for costumers.*
  - La estrategia utilizada por el RENIC para comprender y satisfacer las necesidades y expectativas de sus clientes.
  - La estrategia utilizada por el RENIC para garantizar que las quejas de los clientes son detectadas y resueltas de manera eficaz y eficiente.
  - La estrategia utilizada por el RENIC para recopilar datos estructurados de la percepción de sus clientes, buscando realizar la revisión continua del "*customer relationship management*".
  
- *Developing organizational capacity*
  - La estrategia utilizada por el RENIC para comparar la eficacia y la eficiencia de sus procesos y objetivos clave con los benchmarks externos adecuados.
  - La estrategia utilizada por el RENIC para identificar, formar y desarrollar relaciones con socios externos cuyos productos y servicios complementan a los de los agentes pertenecientes a la Red.
  - La estrategia utilizada por el RENIC para construir una red que soporte y contribuye a los objetivos de su organización.
  
- *Managing with agility*
  - La estrategia utilizada por el RENIC para definir y documentar el marco de los procesos clave necesarios para implementar eficazmente su estrategia.
  - La estrategia utilizada por el RENIC para definir la propiedad y la responsabilidad de administrar sus procesos clave.
  - La estrategia utilizada por el RENIC para identificar, priorizar e implementar mejoras de procesos, incluyendo asegurar que han tenido el impacto deseado en la mejora de la eficacia y eficiencia.
  
- *Leading with vision, inspiration and integrity*
  - La estrategia utilizada por el RENIC para definir y perfeccionar su Visión, Misión y Valores.

- La estrategia utilizada por el RENIC para revisar periódicamente el desempeño en relación con sus objetivos claves y acordar las acciones de mejora apropiadas y las respuestas tácticas a los niveles de desempeño alcanzados.

- *Succeeding through the talent of people*

- La estrategia utilizada por el RENIC para establecer proyectos individuales o de grupo (constructo-nodal) y revisar y mejorar el rendimiento individual.

- La estrategia utilizada por el RENIC para recopilar datos estructurados de percepción las personas involucradas de forma activa a la red buscando la revisión continua de políticas y procesos de recursos humanos.

- *Harnessing creativity and innovation*

- La estrategia utilizada por el RENIC para comprender los cambios y los niveles de rendimiento en el entorno internacional en el que opera.

- La estrategia utilizada por el RENIC para garantizar que las personas, tanto dentro como fuera de su organización, tengan acceso a información precisa, confiable y oportuna que permita la ejecución efectiva de sus procesos clave y el logro de sus objetivos estratégicos.

- *Creating a sustainable future*

- La estrategia utilizada por el RENIC para determinar, gestionar y minimizar el impacto de sus operaciones en el medio ambiente.

- La estrategia utilizada por el RENIC para comprender y maximizar su contribución a la sociedad, ya sea localmente o internacionalmente.

4. Análisis del contexto actual del ecosistema de ciberseguridad en España dentro del marco I+D+i.

- ¿Considera usted que existe la necesidad de implementar un sistema de gestión de calidad en los procesos I+D+i de la red de excelencia RENIC?

- ¿Considera usted que el ecosistema de ciberseguridad en España en el marco I+D+i cuenta con las facultades para implementar un sistema de gestión de la calidad?

- ¿Conoce usted la agrupación AEI ciberseguridad? ¿En qué se diferencian el RENIC y esta agrupación?

**Cierre.**

5. Retos por venir al ecosistema de ciberseguridad de España en el marco I+D+i.

- Presupuesto nacional de ciberseguridad en el marco I+D+i. (Financiación de la UE)

- Plan específico de I+D+i de ciberseguridad en España.

## Anexo VII. Comunicación del RENIC aprobando el estudio.



Correo :: Re: RENIC - Google Chrome

Universitat Politècnica de València [ES] | <https://webmail.upv.es/imp/dynamic.php?page=message&buid=1632&mailbox=S>

← Responder ▾   ➔ Reenviar ▾   🗑 Eliminar

**Re: RENIC** ☰ Ver origen  
⬇ Guardar  
📎 Ver todas las partes

Fecha: 15/03/17 (01:44:32 CEST)  
De: ARTURO RIBAGORDA GARNACHO  
Para: Victor Vera  
Cc: Fernando Raimundo Gonzalez Ladron de Guevara

✉ Ha redirigido este mensaje el 16/03/17 17:57:58 a: [Redacted]

📎 Texto (14 KB) ⬇ 🖨

Estimado Víctor

Siento la demora en responder pero tengo un mes de marzo muy complicado.

En todo caso, después de consultarlo con algunos miembros de la Red, le autorizamos a usar los resultados de la encuesta, bajo condición de hacer notar que RENIC se creo el pasado julio (hasta hace unos días no hemos tenido registro como asociación) y es por tanto una entidad aún en proceso de desarrollo.

También deseamos que nos proporcione los resultados de su trabajo.

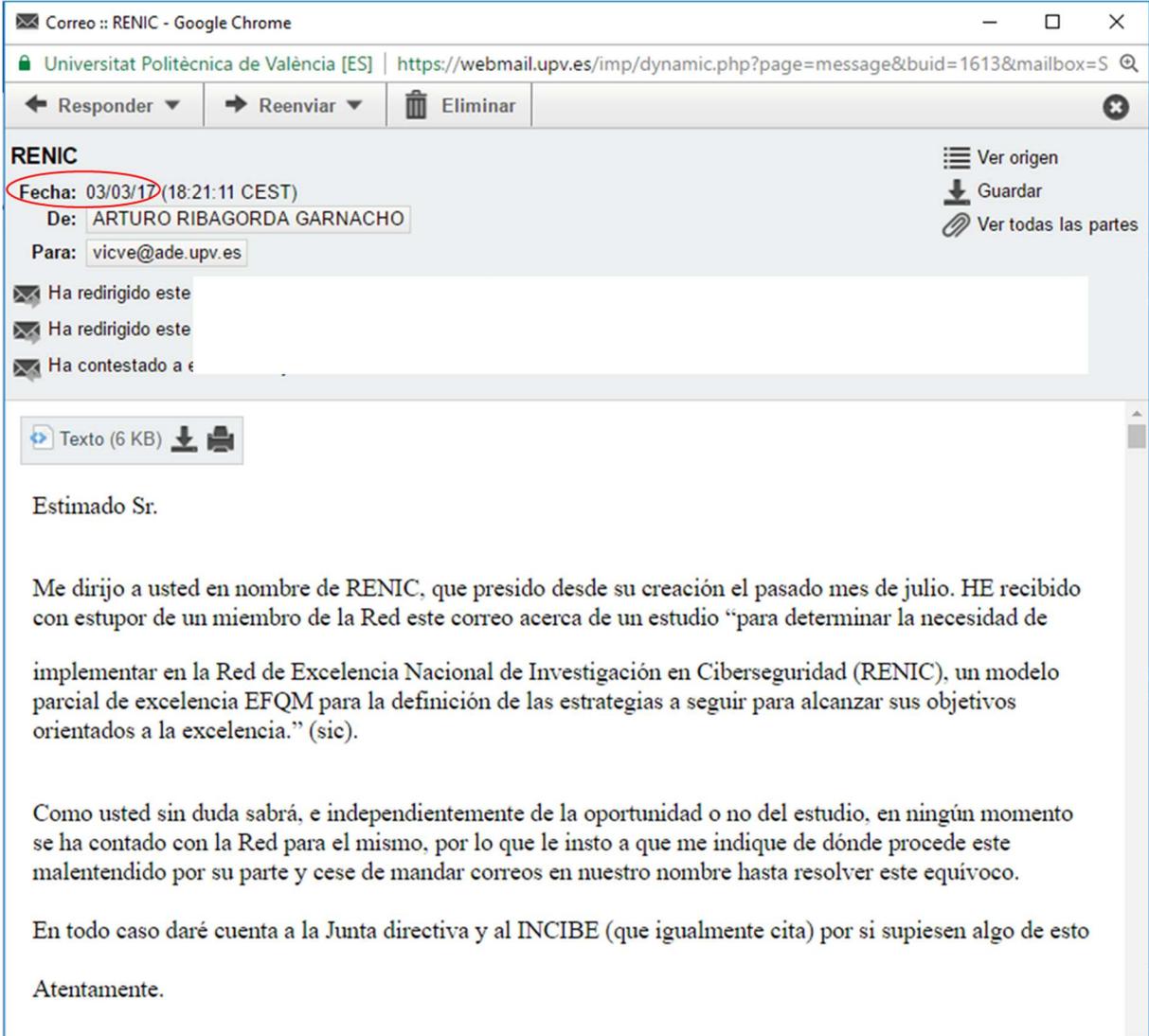
Un saludo y mucha suerte este trabajo.

Arturo Ribagorda  
Grupo COSEC  
[www.seg.inf.uc3m.es](http://www.seg.inf.uc3m.es)  
Departamento de Informática  
Universidad Carlos III de Madrid

---

AVISO LEGAL

## Anexo VIII. Eventualidades suscitadas durante la aplicación del cuestionario.



Correo :: RENIC - Google Chrome

Universitat Politècnica de València [ES] | <https://webmail.upv.es/imp/dynamic.php?page=message&buid=1613&mailbox=S>

← Responder ▾ → Reenviar ▾ 🗑 Eliminar

**RENIC** ☰ Ver origen

Fecha: 03/03/17 (18:21:11 CEST) ⬇ Guardar

De: ARTURO RIBAGORDA GARNACHO 📎 Ver todas las partes

Para: vicve@ade.upv.es

✉ Ha redirigido este  
✉ Ha redirigido este  
✉ Ha contestado a e

📎 Texto (6 KB) ⬇ 🖨

Estimado Sr.

Me dirijo a usted en nombre de RENIC, que presido desde su creación el pasado mes de julio. HE recibido con estupor de un miembro de la Red este correo acerca de un estudio “para determinar la necesidad de implementar en la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), un modelo parcial de excelencia EFQM para la definición de las estrategias a seguir para alcanzar sus objetivos orientados a la excelencia.” (sic).

Como usted sin duda sabrá, e independientemente de la oportunidad o no del estudio, en ningún momento se ha contado con la Red para el mismo, por lo que le insto a que me indique de dónde procede este malentendido por su parte y cese de mandar correos en nuestro nombre hasta resolver este equívoco.

En todo caso daré cuenta a la Junta directiva y al INCIBE (que igualmente cita) por si supiesen algo de esto

Atentamente.

Correo :: Re: RENIC - Google Chrome

Universitat Politècnica de València [ES] | <https://webmail.upv.es/imp/dynamic.php?page=message&buid=74&mailbox=SU5>

← Responder → Reenviar Eliminar

**Re: RENIC**

Fecha: 06/03/17 (22:53:15 CEST)  
De: Victor Vera  
Para: ARTURO RIBAGORDA GARNACHO  
Cc: Fernando Raimundo Gonzalez Ladron de Guevara  
Bcc: eduard606@gmail.com

Ver origen  
Guardar  
Ver todas las partes

**Adjuntos:**  
[Guardar todo]

- Estudio de ecosistema de ciberseguridad en España dentro del marco I+D+i - Cuestionario a agentes relevantes.eml (123 KB)
- Lista de agentes relevantes del ecosistema de ciberseguridad de España.docx (19 KB)
- Instrumento de recolección de datos (Modelo EFQM - RENIC).docx (67 KB)

Texto (5 KB)

Estimado D. Arturo:

Ante todo quisiera manifestar mis más sinceras disculpas por cualquier malentendido generado a la fecha por mi persona.

Debo comenzar aclarando, como se menciona en la comunicación a la cual usted hace referencia, que soy un estudiante del Máster en Gestión de Empresas Productos y Servicios de la Universidad Politécnica de Valencia y el objeto de ésta investigación no es otro que la culminación de mis estudios y la obtención de mi título.

Así mismo, considero importante hacer de su conocimiento que el día 22/02/2017 se envió un comunicado al email: [contacto@renic.es](mailto:contacto@renic.es) notificando la intensión de esta investigación (Ver adjunto) y ante la ausencia de una respuesta oportuna, se contactó a los agentes que dispusieran de un email con acceso público a través del Internet.

Estas acciones, en ningún momento buscaron expresar que se estaba contando con la Red para el desarrollo de la investigación y si fue considerado así por los agentes contactados, estoy en toda la disposición de esclarecer este malentendido de la manera que usted lo considere oportuno.

Finalmente, en aras de lograr un feliz término de mi TFM, solicito respetuosamente me permita continuar el desarrollo de esta investigación, ya que sin su beneplácito no tendría mucho sentido continuar la recolección de datos en los agentes de la red.

Atentamente.  
Víctor E. Vera Pinto.

## **BIBLIOGRAFIA**

---

- Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, 22(4), 308–313. [http://doi.org/10.1016/S0167-4048\(03\)00407-3](http://doi.org/10.1016/S0167-4048(03)00407-3)
- Araújo, M., & Sampaio, P. (2014). The path to excellence of the Portuguese organisations recognised by the EFQM model. *Total Quality Management & Business Excellence*, 25(5–6), 427–438. <http://doi.org/10.1080/14783363.2013.850810>
- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. <http://doi.org/10.1016/j.comnet.2010.05.010>
- Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. *NSPW '01 Proceedings of the 2001 Workshop on New Security Paradigms*, 97–104. <http://doi.org/10.1145/508185.508187>
- Calvo-Mora, A., Navarro-García, A., Rey-Moreno, M., & Periañez-Cristobal, R. (2016). Excellence management practices, knowledge management and key business results in large organisations and SMEs: A multi-group analysis. *European Management Journal*, 34(6), 661–673. <http://doi.org/10.1016/j.emj.2016.06.005>
- CCN. (2016). Resumen ejecutivo.
- Cendoya, A. (2016). *National Cyber Security Organisation: SPAIN*. Tallinn. Retrieved from [https://ccdcoe.org/sites/default/files/multimedia/pdf/CS\\_organisation\\_SPAIN\\_092016.pdf](https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SPAIN_092016.pdf)
- CNSS. (2010). National Information Assurance Glossary. *CNSS Instruction No. 4009, CNSSI*

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

No.(4009).

Du, Z. C., Yao, D. L., & Hu, Y. (2012). Application of EFQM-Based Excellence Model in PPP Projects. In *Advanced Building Materials and Sustainable Architecture* (Vol. 174, pp. 2957–2965). Trans Tech Publications.  
<http://doi.org/10.4028/www.scientific.net/AMM.174-177.2957>

EFQM. (2012). EFQM Framework Innovation Agencies.

European Commission. (2016). Digital Economy and Society Index.

Fischer, E. A. (2016). Cybersecurity issues and challenges: In Brief. *Cyberspace Threat Landscape: Overview, Response Authorities, and Capabilities*, 12. Retrieved from <http://www.scopus.com/inward/record.url?eid=2-s2.0-84956726297&partnerID=tZOtx3y1>

Ghodousi, A. A. J., & Mansouri, R. A. N. (2016). Can excellence management models encompass “ cleaner production ” and “ sustainable business ” revolution ? ( European Foundation for Quality Management as a case study ). *International Journal of Environmental Science and Technology*, 13(5), 1269–1276. <http://doi.org/10.1007/s13762-016-0948-9>

Gómez-Gómez, J., Martínez-Costa, M., & Martínez-Lorente, Á. R. (2016). Weighting the dimensions in models of excellence – a critical review from a business perspective. *Measuring Business Excellence*, 20(3), 79–90. <http://doi.org/10.1108/MBE-01-2016-0007>

Hernandez-Munoz, L., Torane, M., & Amini, A. (2015). Designing an Innovation Engine Model

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

and a Software Tool to Meet Large Organizations Challenges with SMEs Capabilities, a Pilot Study. *Procedia - Social and Behavioral Sciences*, 195, 251–257.

<http://doi.org/10.1016/j.sbspro.2015.06.356>

INCIBE. Estudio de viabilidad, oportunidad y diseño de una red de centros de excelencia en I+D+i en ciberseguridad. (2015).

INCIBE. (2016). Tendencias en el mercado de la Ciberseguridad.

Internet Society. (2012). Some Perspectives on Cybersecurity : 2012. *DNS Security*, 1–22.

ISACA. (2015). Isaca. *Glossary*, 1–103.

ISO/IEC. (2014). ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary. *October*, 3, 38. Retrieved from [http://www.iso.org/iso/catalogue\\_detail?csnumber=42103](http://www.iso.org/iso/catalogue_detail?csnumber=42103)

Jaeger, A., & Matyas, K. (2016). Transformation of the EFQM approach from business towards operations excellence. *Production Engineering*, 10(3), 277–291.

<http://doi.org/10.1007/s11740-016-0665-8>

Jorgenson, D. W., & Vu, K. M. (2016). The ICT revolution, world economic growth, and policy issues. *Telecommunications Policy*, 40(5), 383–397.

<http://doi.org/10.1016/j.telpol.2016.01.002>

Kissel, R. (2013). Glossary of Key Information Security Terms Glossary of Key Information

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en  
España dentro de un marco I+D+i*

Victor E. Vera Pinto

- Security Terms. *Nist, NISTIR 729*(Revision 2). <http://doi.org/10.6028/NIST.IR.7298r2>
- Korff, D. (2015). Cyber Security Definitions – a selection ( US ) National Initiative for Cybersecurity Education ( NICE );, 1–3.
- Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80(3), 541–555.  
<http://doi.org/10.1016/j.techfore.2012.07.002>
- Leeuw, D. (2009). History-of-Information-Security-I-Introduction-aangepast.pdf. In *History-of-Information-Security*.
- Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad : Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Maestría, Programa De Contexto*, 3(4), 161–176. <http://doi.org/http://dx.doi.org/10.18294/relais.2015.161-176>
- Luijff, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *Int. J. Critical Infrastructures*, 9(12), 3–31.
- Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497–1516.  
<http://doi.org/10.1016/j.adhoc.2012.02.016>
- Moreno, J. (2007). Guía para la aplicación del modelo EFQM de excelencia en entidades de acción social.

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en España dentro de un marco I+D+i*

Victor E. Vera Pinto

ONTSI. (2016). Nota de prensa, 1–5.

Pipkin, D. L. (2000). *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc.

Polo Tecnológico Nacional Ciberseguridad, E. N. (2016). Informe de internacionalización de empresas.

Presidencia del Gobierno. (2013). Estrategia de Seguridad Nacional.

Presidencia del Gobierno de España. Estrategia de Ciberseguridad Española (2013). Retrieved from [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES\\_NCSS.pdf](http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf)

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*, 60, 154–176. <http://doi.org/10.1016/j.cose.2016.04.003>

Trott. (2009). *Innovation Management and New product development*.

UK-Cabinet-Office. (2011). The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. [Online] at: <https://www.gov.uk/>, (November), 1–42. <http://doi.org/10.1109/MC.2013.72>

Venter, H. S., & Eloff, J. H. P. (2004). Vulnerability Forecasting-a Conceptual Model. *Comput. Secur.*, 23(6), 489–497. <http://doi.org/10.1016/j.cose.2004.06.005>

*Modelo parcial de excelencia EFQM para el ecosistema actual de la ciberseguridad en  
España dentro de un marco I+D+i*

Victor E. Vera Pinto

Wamala, F. (2008). *The ITU National Cybersecurity Strategy Guide*.

Weber, R. H., & Studer, E. (2016a). Cybersecurity in the Internet of Things: Legal aspects.

*Computer Law & Security Review*, 32(5), 715–728.

<http://doi.org/http://dx.doi.org/10.1016/j.clsr.2016.07.002>

Weber, R. H., & Studer, E. (2016b). Cybersecurity in the Internet of Things: Legal aspects.

*Computer Law & Security Review*. <http://doi.org/10.1016/j.clsr.2016.07.002>

Weber, R. H., & Studer, E. (2016c). Cybersecurity in the Internet of Things: Legal aspects.

*Computer Law & Security Review*, 32(5), 715–728.

<http://doi.org/10.1016/j.clsr.2016.07.002>

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security. Course*

*Technology*. <http://doi.org/10.1016/B978-0-12-381972-7.00002-6>

Y. Cherdantaseva & J. Hilton. (2013). A Reference Model of Information Assurance & Security.

*Proceedings of the 8th ARES Conference 2013 (ARES 2013)*, 1–11.