Cuadernos de Estrategia 185

Ciberseguridad: la cooperación público-privada

Instituto Español de Estudios Estratégicos

Departamento de Seguridad Nacional

MINISTERIO DE DEFENSA

DSN

ieee.es
Instituto Español de Estudios Estratégicos

CESEDEN

Cuadernos de Estrategia 185

Ciberseguridad: la cooperación público-privada

Instituto Español de Estudios Estratégicos

Departamento de Seguridad Nacional

MINISTERIO DE DEFENSA

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
http://publicacionesoficiales.boe.es/

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

http://publicaciones.defensa.gob.es/

© Autores y editor, 2016

NIPO: 083-16-446-2 (edición papel)
ISBN: 978-84-9091-245-4 (edición papel)

Depósito Legal: M-40233-2016
Fecha de edición: marzo 2017
Imprime: Ministerio de Defensa

NIPO: 083-16-447-8 (edición libro-e)
ISBN: 978-84-9091-246-1 (edición libro-e)

Las opiniones emitidas en esta publicación son exclusiva responsabilidad de los autores de la misma.
Los derechos de explotación de esta obra están amparados por la Ley de Propiedad Intelectual. Ninguna de las partes de la misma puede ser reproducida, almacenada ni transmitida en ninguna forma ni por medio alguno, electrónico, mecánico o de grabación, incluido fotocopias, o por cualquier otra forma, sin permiso previo, expreso y por escrito de los titulares del © Copyright.

En esta edición se ha utilizado papel 100% reciclado libre de cloro.

EU Ecolabel www.ecolabel.eu
100%

ÍNDICE

Página

Introducción 11
Luis Joyanes Aguilar

Una visión global de la colaboración público-privada en ciberseguridad .. 13

Capítulo primero

Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0) 19
Luis Joyanes Aguilar

La ciberseguridad en tiempo real 21

El índice mundial de ciberseguridad de la UIT (*ITU*) 22

Clasificación mundial (índice IMC) 23

La cuarta revolución industrial 24

Industria 4.0: origen, evolución y futuro 25
Industria conectada 4.0 26

Las tecnologías disruptivas pilares en la Industria 4.0 y en la ciberseguridad 28

Tendencias en ciberseguridad: un primer avance (2015-2016) 31

Informe de seguridad de la información de Cisco 32

Recomendaciones de Cisco 33

Los ciberriesgos 33
La web profunda, la web invisible (Deep Web) 34
La necesidad de un seguro de ciberriesgos en la empresa 35

La ciberseguridad en la empresa y la empresa ante la ciberseguridad 36
El negocio de la ciberseguridad 37

La ciberseguridad en la industria eléctrica: necesidad de estándares 37

La ciberseguridad en la banca y en el sector financiero (tecnologías financieras de impacto) 39
Tecnologías y empresas Fintech 40
Blockchain 41

La ciberseguridad y la inteligencia artificial 42

Página

IBM Watson 43
Watson for Cyber Security 44
Plataforma de Ciber-Inteligencia de Accenture 44

Robótica y ciberseguridad: cobots, bots y chatbots 45
Robots colaborativos (cobots) 45
***Los asistentes virtuales:* bots *y* chatbots** 46
***Aplicaciones de los* bots** 47
Asistentes virtuales en páginas web de organizaciones y empresas 48
Los* bots*: ¿las nuevas aplicaciones móviles? 48
***La seguridad y los riesgos de los* bots** 49

El nuevo reglamento de protección de datos de la Unión Europea (25 de mayo de 2016) 49
Novedades del nuevo reglamento 50
Recomendaciones de la AEPD sobre el nuevo reglamento 50

Proyecto de colaboración público-privada de la Unión Europea (5 de julio de 2016) 51

Directiva de ciberseguridad (*NIS*) de la Unión Europea (6 de julio de 2016) 52

El escudo de privacidad Unión Europea-Estados Unidos (12 de julio de 2016) 53

La formación en ciberseguridad y en sus tecnogías disruptivas 54
Los nuevos roles profesionales 55

Los datos: presente y futuro de la ciberseguridad 57

La ciberseguridad en América Latina y Caribe 57
Tendencias de seguridad cibernética en América Latina y el Caribe (junio 2014) 58
Ciberseguridad 2016 en América Latina y Caribe (marzo 2016) 59

Conclusiones: tendencias en ciberseguridad 60
Tendencias TIC de INCIBE (2016). Julio 2016 60
Nuevos escenarios y desafíos de la seguridad. Telefónica (septiembre de 2016) 61
Otras tecnologías de impacto en el futuro de la ciberseguridad analizadas 61

Estudios de ciberseguridad 63

Bibliografía de consulta 64

Capítulo segundo

Crisis y ciberespacio: hacia un modelo integral de respuesta en el Sistema de Seguridad Nacional 65
Joaquín Castellón Moreno
María Mar López Gil

Introducción 67

La lucha por el control del ciberespacio 70

De la gestión de incidentes a la gestión de crisis en el ciberespacio 72

Los ciberataques del siglo XXI y sus consecuencias 74
El soldado de bronce de Tallin 74
La ralentización del Programa nuclear iraní 75
Ataques a los servicios esenciales en la Europa del Este 76
Los ataques silenciosos y el robo de información 77

Página

Las oportunidades del ciberespacio para la amenaza terrorista 78
Ataques a la reputación e influencia política 79
Las amenazas al sector privado 80
Ataques con efectos cinéticos 82

La gestión de crisis en el Sistema de Seguridad Nacional 82

Colaboración público-privada y gestión de crisis de ciberseguridad en el Sistema de Seguridad Nacional 85

De la acción a la puesta en práctica. El ejercicio *Cyber Europe* 91

Conclusiones y retos 93

Capítulo tercero

Análisis de las ciberamenazas 97
Aníbal Villalba Fernández
Juan Manuel Corchado Rodríguez

Introducción 99

Las ciberamenazas en el contexto de los riesgos globales 102

Elementos esenciales en el análisis de las amenazas 105

Evolución tecnológica y ciberseguridad 106

Ciberamenazas, agentes y objetivos 110
Los agentes de las ciberamenazas 111
Criterios de determinación del nivel de peligrosidad de los ciberincidentes 119
Herramientas de las amenazas 120
Tendencias de amenazas globales de ciberseguridad 125

Ciberincidentes en España 131

Conclusiones 136

Capítulo cuarto

El intercambio de información de ciberamenazas 139
Miguel Rego Fernández
Pedro Pablo Pérez García

Situación actual 141
Necesidad de intercambiar información de amenazas e incidentes 141
Inhibidores y habilitadores para la compartición de información de amenazas 141
Barreras en el intercambio de información derivados de aspectos legales 142
Barreras en el intercambio de información derivados de falta de confianza 143
Insuficiente interés por parte de las partes 144
Barreras de carácter técnico 144
***Beneficios y habilitadores en el* Information Sharing** 145
Marco normativo y legislativo aplicable en Europa y España 146
Áreas para una cooperación efectiva en el intercambio de amenazas 151
***Los problemas de la normalización: iniciativas privadas* vs *estándares* de facto** 154
Datos a intercambiar 154
Métodos de intercambio 155
Formatos de intercambio de datos de amenazas 156
OpenIOC 157
CybOX, STIX, TAXII 157

Página

OTX 161
MISP 161
Análisis de requisitos de los actores del ecosistema público-privado para el intercambio de amenazas 163
Empresas, Administraciones y usuarios/ciudadanos 163
ISAC* vs *ISAO 163
Fabricantes y proveedores de servicios de inteligencia 165
Organismos oficiales* (CERT, *CSIRT y agencias públicas) 165
El caso norteamericano: Cyber Threat Intelligence Integration Center (CTIIC) 166

Conclusiones y Recomendaciones 168

Bibliografía de consulta 169

Capítulo quinto

Cooperación público-privada en la protección de infraestructuras críticas 171
Fernando Sánchez Gómez
Justo López Parra

Introducción 173

Un poco de historia 174
BlackEnergy 176
Stuxnet 177
Ciberataque a Estonia 2007 179
Titan Rain 179

Pilares de la colaboración en la protección de las infraestructuras críticas 180

El sistema de planificación PIC y su encaje con la ciberseguridad 184
Normativa PIC, colaboración público-privada y ciberseguridad 184
El Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC) 188
Los Planes Estratégicos Sectoriales (PES) 192
Los Planes de Seguridad del Operador (PSO) 195
Los Planes de Protección Específicos (PPE) 196
Los Planes de Apoyo Operativo (PAO) 198

Herramientas para la colaboración 199
Apoyo frente a incidentes 199
El equipo de respuesta a incidentes cibernéticos de seguridad e industria (CERTSI_) 201
La Oficina de Coordinación Cibernética del Ministerio del Interior 202
Alerta temprana e intercambio de información 204
Ciberejercicios 207
Acuerdos de colaboración 209
Controles recomendados 210

Bibliografía 213

Capítulo sexto

La cooperación público-privada en el fomento de la cultura de ciberseguridad 217
Gregorio Miguel Pulido Alonso
Rafael Rosell Tejada

Introducción 219

El eslabón más débil de la cadena 220

Ciberresiliencia y concienciación en ciberseguridad 223

Página

Iniciativas existentes ... 224
En España ... 224
Dentro del sector privado ... 231
Fuera del entorno laboral ... 233
A nivel multinacional ... 234
Como parte de la ciberdefensa ... 235
Programas, planes, campañas de concienciación ... 237
Cooperación público-privada para la concienciación en ciberseguridad ... 240
Experiencias y buenas prácticas ... 243
Un ejemplo concreto ... 244
Conclusiones ... 245

Capítulo séptimo

I+D+i y ciberseguridad: análisis de una relación de interdependencia ... 247
Aurelio Hinarejos Rojo
José de la Peña Muñoz

Introducción ... 249
Investigación, desarrollo e innovación en ciberseguridad ... 253
La investigación y el desarrollo ... 254
Innovación ... 260
Necesidad de una actuación específica de I+D+i en ciberseguridad ... 262
La inversión en I+D+i en ciberseguridad ... 268
El papel de la colaboración público-privada en el proceso de I+D+i ... 275
Iniciativas foráneas ... 277
Iniciativas supranacionales ... 278
España ... 279
Retos, riesgos y oportunidades ... 280
Interdependencia entre innovación y ciberseguridad ... 283
Conclusión ... 286

Capítulo octavo

Capacitación profesional y formación especializada en ciberseguridad ... 291
Óscar Pastor Acosta
José Javier Martínez Herráiz

Introducción ... 293
Escasez de profesionales en ciberseguridad ... 295
Iniciativas de organismos públicos para la formación y certificación profesional en ciberseguridad ... 300
National Cybersecurity Workforce Framework ... 301
CESG Certified Professional Scheme ... 306
DoD 8570.01-M ... 312
CCN/INAP - Esquema Nacional de Certificación de Profesionales en Ciberseguridad ... 316
SEPE - Certificado de Profesionalidad en Seguridad Informática ... 319
Iniciativas privadas de formación y certificación en ciberseguridad ... 321
ISACA-CSX (Cybersecurity Nexus) ... 321
(ISC)²-CISSP (Certified Information Systems Security Professional) ... 325
SANS/GIAC ... 331
EC-Council - CEH (Certified Ethical Hacker) ... 336

Página

Conclusiones 338

Bibliografía 342

EPÍLOGO

Presente y futuro de la ciberseguridad: el impacto y la necesidad de la colaboración público-privada 351
Luis Joyanes Aguilar

La ciberseguridad en la transformación digital 351

La concienciación en ciberseguridad 352

El futuro de la ciberseguridad 352

El decálogo de ciberseguridad FTF & Fundación Bankinter 353

El decálogo de ciberseguridad de INCIBE 354

Ciberseguridad 4.0 355

Composición del grupo de trabajo 357

Cuadernos de Estrategia 359

Capítulo octavo

Capacitación profesional y formación especializada en ciberseguridad

Óscar Pastor Acosta
Gerente de Seguridad
Isdefe

José Javier Martínez Herráiz
Director de la Cátedra Amaranto de Seguridad Digital
Universidad de Alcalá de Henares

Resumen

En el presente capítulo se abordará uno de los aspectos donde mayor puede llegar a ser la colaboración público-privada en materia de ciberseguridad y ciberdefensa: la necesidad de capacitar de manera adecuada a los profesionales especialistas en esta materia. Veremos cómo esta necesidad es casi un imperativo, el de la colaboración, al continuar aumentando la brecha entre la necesidad de profesionales y la oferta de los mismos.

Empezaremos, precisamente, analizando esta escasez de profesionales en todo el mundo y las cotas de preocupación que está alcanzando, tanto a nivel de los Estados y sus políticas nacionales como en el sector privado.

Continuaremos estudiando las iniciativas procedentes de organismos públicos en lo que respecta a la formación, certificación y acreditación de conocimientos en ciberseguridad, terminando con las procedentes del sector privado, en este caso, más centradas en la importancia de las certificaciones como garantía y aseguramiento de calidad y nivel.

El presente análisis no pretende hacer una descripción y búsqueda exhaustiva ni una descripción pormenorizada de todas las iniciativas en esta temática, sino centrarse en aquellas que nos parecen más relevantes y significativas. Quedan, manifiestamente, también fuera del mismo las innumerables iniciativas académicas, tanto públicas como privadas.

La otra iniciativa europea que va a requerir la alineación de todos los esquemas de cualificaciones nacionales y locales es la nueva clasificación oficial laboral europea para todos los sectores, *ESCO* (*European Skills, Competences, Qualifications and Occupations*)[100], aún pendiente de publicarse en 2017.

Esta nueva clasificación laboral va a ser de uso obligatorio para todos los servicios públicos de empleo y para los recursos europeos como el portal EURES, además de promoverse como estándar para los portales privados, y estará traducida a todos los idiomas oficiales de la Unión Europea.

En el ámbito sectorial de las TIC se ha generado un nuevo catálogo de ocupaciones con ciento diez puestos y su correspondiente descripción y lista de habilidades y conocimientos, tanto esenciales como opcionales. En el ámbito de la seguridad se distinguen los puestos de *CISO* (*Chief Information Security Officer*), administrador de seguridad TIC, consultor de seguridad TIC, gerente (*manager*) de seguridad TIC, técnico de seguridad TIC y *hacker* ético. Al igual que en *eCF*, existe una buena cantidad de otras ocupaciones con habilidades y conocimientos relacionados con la seguridad.

Actualmente estos modelos están generando importantes expectativas, pero también la necesidad de buscar su consistencia para permitir que los servicios para candidatos a empleos, reclutadores y formadores sean completos y sólidos. En ese sentido, los resultados de proyectos europeos como *eSkills Match*[101], con un sistema de ayuda en el manejo de los modelos, y *eCF Council*[102] permitirán mejorar este aspecto de forma práctica, incluyendo la conexión con el cuerpo europeo de conocimientos en TIC[103].

En todo caso, parece existir un consenso a nivel mundial de que dicha escasez de profesionales de las TIC y, en particular, de la ciberseguridad tendrá implicaciones negativas en la seguridad nacional, impactando gravemente tanto en entidades del sector público como del privado.

En este sentido, y en un ámbito nacional, es pertinente resaltar el documento y proyecto del Instituto Nacional de Ciberseguridad (INCIBE) de 2016 denominado «Punto de partida al modelo de gestión y seguimiento del talento

[100] Comisión Europea, «ESCO (European Skills, Competences, Qualifications and Occupations)», accedido 2 de noviembre de 2016, https://ec.europa.eu/esco/portal/home

[101] European Commission Directorate General for Communications Networks, Content & Technology (DG CONNECT), «Proyecto e-Skills Match», accedido 2 de noviembre de 2016, http://www.eskillsmatch.eu/

[102] eCF Council, «eCF ALLIANCE , qualifications and skills for the ICT industry», accedido 2 de noviembre de 2016, http://media.wix.com/ugd/71d4ca_273ca002273242c28d1557836c68cbcc.pdf

[103] European Commission - DG Internal Market, Industry, Entrepreneurship and SMEs, Capgemini Consulting, y Ernst & Young, «The European Foundational ICT Body of Knowledge - Version 1.0», 22 de febrero de 2015, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=925&PortalId=0&TabId=353