ÍNDICE

¿Por qué una conciencia nacional de *ciberseguridad*? 9

Bibliografía 27

Capítulo primero
Principios de una conciencia nacional de *ciberseguridad* 35
Por José Tomás Hidalgo Tarrero

Guerra total, guerra asimétrica y *ciberguerra* 35

Antecedentes de conciencia nacional de *ciberseguridad* 38

Principios en los que se debe basar la conciencia nacional de *ciberseguridad* 42
- ***Conocimiento de las amenazas y los riesgos y asumirlos*** 42
- ***Notificación por los usuarios de los errores e incidencias sufridos*** 44
- ***Información por los responsables de seguridad de los sistemas informáticos de los ISP, de las instituciones y empresas a los usuarios, miembros, empleados y clientes*** 46
- ***Formación de todos, cada uno en el nivel que corresponda, en ciberseguridad*** 47
- ***Adaptabilidad de usuarios, instituciones y empresas a las circunstancias cambiantes del ciberespacio*** 49
- ***La base de los principios de conciencia nacional de «ciberseguridad»*** 50

Requisitos necesarios para poderlo hacer 52

Participación de las instituciones de la sociedad civil 61

Conclusiones 67

Bibliografía 69

Capítulo segundo
Conciencia ciudadana de *ciberseguridad* 71
Por José Manuel Roldán Tudela

Introducción 71

El ciberespacio y la persona 73
- ***El ciberespacio*** 73
  - Existencia 73
  - Modelo 74

Página

La persona ... 77
Datos personales ... 77
Identidad digital ... 80
Ciudadano digital ... 83

Los riesgos ... 84
Análisis centrado en los riesgos ... 84
Atacantes ... 87

Víctimas ... 92
Activos ... 93
Amenazas ... 97
Disminución del riesgo ... 114

Conciencia de *ciberseguridad* ... 118
Grados ... 118
Los sujetos ... 120
Los actores ... 121
El objeto ... 122
Los medios ... 124

Conclusiones ... 127

Bibliografía ... 132

Capítulo tercero
Concienciación en las administraciones públicas ... 137
Por Luis Jiménez Muñoz

Toma de conciencia y percepción del riesgo ... 137
Las vulnerabilidades ... 143
El nuevo enfoque en la gestión de riesgos ... 146

Toma de conciencia de lo que hay que proteger ... 148
Las políticas de seguridad de la información ... 148
Principios de seguridad ... 149
El Esquema Nacional de Seguridad ... 152

Las responsabilidades básicas del personal de la Administración ... 158
La organización de seguridad ... 159
Las responsabilidades y los riesgos ... 164

Las normas y los procedimientos ... 166
Ejemplo del contenido de una norma general de utilización de los recursos y sistemas de información de un organismo de la Administración ... 169

Información y concienciación ... 171

La formación del personal de la Administración ... 173
Instituto Nacional de Administración Pública ... 175
Federación Española de Municipios y Provincias ... 178
Centro Criptológico Nacional ... 178
Contenido de la oferta formativa del CCN en 2011-2012 ... 181

Bibliografía ... 182

Capítulo cuarto
La conciencia de *ciberseguridad* en las empresas ... 185
Por Oscar Pastor Acosta

Introducción ... 185
Contenido ... 187

Las empresas en el ciberespacio ... 188
Activos de las empresas en el ciberespacio ... 188
Activos intangibles: propiedad intelectual, reputación y marca ... 188

Página

Infraestructuras críticas 194
Los servicios esenciales y las infraestructuras críticas 194
Ciberdependencia de las infraestructuras críticas 196
Amenazas a las empresas desde el ciberespacio 198
Amenazas a la propiedad intelectual 198
Amenazas a la reputación y marca 203
Amenazas a las infraestructuras críticas 209
Principales vulnerabilidades para las empresas de las tecnologías del ciberespacio 212
Cloud computing 212
Principales vulnerabilidades de la computación en la nube 215
Big data 219
Principales vulnerabilidades del *big data* 220
«Consumerización» y BYOD 222
Principales vulnerabilidades del BYOD 224
Redes sociales 225
Principales vulnerabilidades de las redes sociales 226
Vulnerabilidades asociadas a la presencia corporativa en redes sociales 227
Vulnerabilidades asociadas al uso por parte de los empleados de las redes sociales 228
Buenas prácticas de seguridad para las empresas en el ciberespacio 229
Uso de productos certificados 229
La norma «Common Criteria» 229
Aspectos evaluados en un proceso de certificación «Common Criteria» 230
Consumo de productos certificados CC 233
La norma CC en la cadena de suministro 236
Buenas prácticas para la gestión de la seguridad de la información 237
ISO 27000: Sistemas de gestión de la seguridad de la información 237
«20 Critical Security Controls» 239

La concienciación de *ciberseguridad* en las empresas 242
Programas de formación y concienciación 242

Bibliografía 246

Capítulo quinto
Cooperación internacional en temas de ciberseguridad 255
Por Emilio Sánchez de Rojas Díaz

Introducción 255

Comienza la amenaza transfronteriza 256
Dominios conectados globalmente 257
Spamhaus 261
El tratamiento de la «ciberdefensa» en las políticas de defensa 261

Los principales actores nacionales 262
Posición respecto a la cooperación internacional 264
Alemania 264
EE. UU. 265
Rusia 265
Francia 267
China 268
Unión Europea 270

Página

El papel de las organizaciones internacionales 271
ONU 271
Antecedentes 271
La seguridad de la información en la ONU 273
OTAN 276
Consejo de Europa 280
OSCE 281
Caso de análisis: la Unión Europea 284
Caso de análisis: los EE. UU. 289
Conclusiones 300
Bibliografía 301

Conclusiones de una conciencia de *ciberseguridad* y *ciberdefensa* 307
Bibliografía 331

Composición del grupo de trabajo 335

Relación de Monografías del CESEDEN 337