MARÍA ÁNGELES CABALLERO
DIEGO CILLEROS SERRANO

EL LIBRO DEL HACKER

EDICIÓN 2022

ANAYA MULTIMEDIA

EL LIBRO DEL HACKER

EDICIÓN 2022

EL LIBRO DEL HACKER

EDICIÓN 2022

MARÍA ÁNGELES CABALLERO
DIEGO CILLEROS SERRANO

ANAYA MULTIMEDIA

Responsable editorial: Víctor Manuel Ruiz Calderón

Diseño de cubierta: Celia Antón Santos

Ilustraciones de cubierta, portadillas y de páginas 3, 26, 36, 147, 152, 169, 177, 403, 485, 487: © 2021 iStockphoto L.P. /Getty Images

Primera edición electrónica 2021

Todos los nombres propios de programas, sistemas operativos, equipos hardware, etc. que aparecen en este libro son marcas registradas de sus respectivas compañías u organizaciones.

Reservados todos los derechos. El contenido de esta obra está protegido por la Ley, que establece penas de prisión y/o multas, además de las correspondientes indemnizaciones por daños y perjuicios, para quienes reprodujeren, plagiaren, distribuyeren o comunicaren públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la preceptiva autorización.

© EDICIONES ANAYA MULTIMEDIA (GRUPO ANAYA, S.A.), 2022
Juan Ignacio Luca de Tena, 15. 28027 Madrid
ISBN: 978-84-415-4444-4
Edición digital sobre la 1.ª edición impresa 2021

A Ariadna, nuestra hija, por ser nuestra inspiración,
por toda esa ternura que desprendes y tus maravillosas sonrisas.
Nos has hecho entender lo que es el amor incondicional, infinito, indescriptible.
Por toda una vida llena de alegrías que nos espera junto a ti. ¡Te queremos, bombón!

Agradecimientos

Queremos agradecer este libro a nuestras familias y amigos que siempre nos han apoyado cuando hemos hecho este tipo de proyectos, así como expresar nuestro agradecimiento por el respaldo recibido por nuestros compañeros de trabajo, que nos han asesorado y apoyado en todo momento y sabemos que lo seguirán haciendo en un futuro.

La ciberseguridad, tanto desde un punto de vista más técnico como más conceptual, es un mundo complejo y en constante evolución, por lo que siempre tenemos que estar actualizándonos y aprendiendo nuevos conceptos, técnicas y herramientas, lo que nos lleva a pasar muchas horas de estudio y análisis. En esos momentos de retiro nunca nos falta el apoyo de nuestros seres queridos, que nos ayudan y comprenden. Por todo ello, les damos las gracias y esperamos que sigan soportando los nuevos retos que seguro llevaremos a cabo en el futuro.

Desearíamos expresar nuestra máxima gratitud a todos los lectores de este libro, ya que sin ellos esto no sería posible. Esperamos aportar conocimientos de gran utilidad e innovadores, para que el lector aprenda con cada página, al igual que nosotros lo hemos hecho durante el desarrollo de la obra.

Sería desleal por nuestra parte no acordarnos y agradecer, además, a todos los cibernautas que desarrollan y aportan su conocimiento de manera desinteresada en Internet, a todos los foros de seguridad y *hacking* en la red. Gracias también a Internet y a sus creadores por haber cambiado el mundo en el que vivimos y que nos permite intercambiar conocimientos sin importar el lugar ni el tiempo.

Para terminar, agradecer de manera muy especial a Anaya Multimedia por darnos una nueva oportunidad y por el interés y ganas que han puesto en este libro, confiando en la materia que trata. También dar las gracias al editor, Víctor Manuel Ruiz, que siempre pone todos sus medios para ayudarnos en la realización de un nuevo libro.

Por último, queríamos agradecer la inestimable aportación en el libro de Pilar Gandía Herrero, doctora en Psicología, por ayudarnos a entender cuál es la psicología del cibercriminal en un capítulo novedoso y muy didáctico.

A todos ellos muchas gracias.

Sobre los autores

María Ángeles Caballero Velasco



María Ángeles Caballero Velasco cuenta con más de 10 años de experiencia en el sector de la ciberseguridad. Actualmente es *Head of Cybersecurity* para una de las principales entidades del Banco Santander en el ámbito de CISO (Chief Information Security Officer). Es ingeniera en Informática Técnica de Gestión y licenciada en Administración y Dirección de Empresas por la Universidad Carlos III de Madrid. También ha cursado el Máster Universitario en Seguridad de las TIC por la UEM y el Máster en Design Thinking por el MIT. Posee múltiples certificaciones como CISSP, SSCP, CEH o PMP y tiene numerosas publicaciones en libros, revistas y foros, habiendo publicado 7 libros de ciberseguridad hasta la fecha. Ha participado en múltiples seminarios, conferencias y cursos, dado que le entusiasma la concienciación y la formación. Finalmente, su pasión por el comportamiento y la cognición humana le ha llevado a estar cursando actualmente el Grado de Psicología por la UNED y a certificarse como *coach profesional* con la escuela americana IPEC.

`es.linkedin.com/in/angelescaballero`.

Diego Cilleros Serrano



Es ingeniero superior de Telecomunicaciones por la Universidad Carlos III de Madrid y estudiante de Grado de Criminología por la Universidad Internacional de La Rioja. Su experiencia profesional ha estado siempre ligada al mundo de las redes de datos y de la ciberseguridad, trabaja actualmente como gerente *senior* de ciberseguridad en el área Cyber Risk Services de Deloitte España y es responsable de un equipo cercano a las 100 personas dedicado a las arquitecturas de seguridad y a la seguridad *cloud*. Posee diferentes certificaciones de ciberseguridad que complementan su experiencia, como Offensive Security Certified Professional (OSCP), Certified SCADA Security Architect (CSSA), CISSP, CCSP, CSX y CISA, y algunas relacionadas con AWS y Azure, entre otras. Ha participado en diferentes seminarios y cursos, y es coautor de diferentes publicaciones sobre ciberseguridad.

`es.linkedin.com/in/diegocilleros`.

Sobre los colaboradores directos

Pilar Gandía Herrero

Doctora en Psicología por la Universidad de Murcia, y profesora en el departamento de Psicología Básica y Metodología de esta universidad. Cuenta con 10 años de experiencia en su ámbito. Es psicóloga forense y perito en ejercicio privado. Realizó el Máster en Psicología de la Intervención Social, intensificando su formación en la psicología jurídica y forense. Además, ha sido formadora en varios cursos relacionados con esta temática, y actualmente imparte docencia en el grado de Psicología, y en los Másteres Oficiales de Abogacía y de Psicología Jurídica. Compagina el desarrollo privado de la profesión y la docencia con la investigación, siendo sus principales aportaciones al ámbito de la psicología jurídica.

Índice de contenidos

Agradecimientos 6
Sobre los autores 7
Sobre los colaboradores directos 8

INTRODUCCIÓN **19**

Nuevas tecnologías, nuevos retos 19
Objetivos del libro 20
Organización del libro 21

1. EL MUNDO DIGITAL ES INSEGURO **25**

Tiempos de incertidumbre 25
Grandes cifras 28
Filosofía *hacker* y argot 35
White hat, *sneaker* o hacker ético 37
Black hats o *crackers* 38
Grey hats 38
Insiders 38
Script kiddies 39
Phreakers 39
Conceptos y enfoques 39
Conceptos básicos de seguridad: CIA 40
Triángulo de seguridad, funcionalidad y facilidad de uso 40
Enfoque de perímetro de seguridad 41
Zero Trust 42
Defensa en profundidad o enfoque de seguridad por capas 43
Metodologías y estándares en ciberseguridad 43
NIST Cybersercurity Framework 43

Recursos de seguridad *online* 50
Leyes y normativas de aplicación nacional 52
Estrategia de Ciberseguridad Nacional 53
Ley de Protección de Infraestructuras Críticas 55
Instituciones 55

2. CIBERAMENAZAS 59

Trabajando en remoto de manera segura 59
Threat actors 60
Panorama de las ciberamenazas 61
Phishing e ingeniería social 63
Cómo protegernos 70
Malware y *ransomware* 72
SIM Swapping 81
Errores, entrega incorrecta y mala configuración 84
Supply Chain Attack 87
Distributed Denial of Service o denegación de servicio distribuido 92
Cryptojacking 96
Uso de credenciales robadas 100
La cadena de ataque 103
Pasos y etapas 104
Cyber Kill Chain 107
MITRE ATT&CK™ 108

3. CIBERGUERRA 113

Introducción 113
Ciberguerra, ciberespionaje y ciberataques 115
Historia de la ciberguerra 115
Stuxnet, "el *malware* más inteligente jamás visto" 118
¿Quién creó Stuxnet? 119
Algo sobre su historia 119
Propagación de Stuxnet 121
APT & *Targeted Attacks* 122
Vías de infección 123
¿Quién crea los APT? 123
Ejemplo práctico de un APT y metodología de análisis 124
Detección del APT 125
Análisis del correo electrónico original 126
Análisis del adjunto malicioso 132
Análisis del código fuente del fichero 132
Reproducción del ataque 136

4. HACKER MINDSET 141

Término *hacker* 141
Introducción 141
Desde la psicología 142
¿Hablamos de estereotipos o de perfiles criminales? 142
El cibercriminal como agente del delito 145
Refuerzo emocional 148
¿Quiénes son los más vulnerables? 152
Influencia y persuasión 153
Actores de amenazas 159
Motivaciones y sofisticación 160
Entendiendo las motivaciones 162
Ciberterrorismo 165
Crimen organizado 166
Hacktivistas 168
Lobos solitarios 171
Insiders 174

5. ARQUITECTURAS DE RED Y DATOS: DEFENSA Y OFENSIVA 181

Introducción 181
Conceptos de red y comunicaciones 182
Modelo OSI vs. Modelo TCP/IP 182
IPv4 185
IPv6 191
TCP 195
Consideraciones de seguridad sobre protocolos 200
Hardware de red 202
Arquitecturas de red 204
La seguridad en la red de datos 205
Firewalls 206
VPN 208
DLP 209
Arquitecturas de seguridad 210
Otros elementos de seguridad 212
Zero Trust 215
Protección de infraestructuras en la nube 216
Próximos enfoques: ZTNA y SASE 217
Ofensiva en la red 220
Ataques a nivel de red 220
Wireless: Wi-Fi 223
VoIP 248

6. MUNDO INDUSTRIAL E IOT 265

Industria 4.0 265
Conceptos y arquitectura de SCADA 267
Seguridad en entornos SCADA 271
Desmitificando los ataques sobre SCADA 274
Breve introducción a IoT 281
El reto de la seguridad IoT 282

7. HACKING WEB Y SEGURIDAD EN MICROSERVICIOS 285

Introducción 285
OWASP Top 10 286
WebGoat 288
Metodología 289
Proxy web 290
Mapeado web 291
Análisis automático de vulnerabilidades web 293
Inyección 299
Inyección de comandos 299
SQL Injection 302
Cross-Site Scripting (XSS) 311
XSS almacenado o persistente 312
XSS reflejado 312
XSS basado en el DOM 313
Servidor vs. Cliente 313
Puesta en práctica 313
Inclusión de ficheros 317
LFI 318
RFI 321
Otros controles 323
Sistemas de gestión de contenidos 324
Análisis de Wordpress 325
Microservicios y contenedores 332
Tecnología de contenedores 335
Docker 336
Seguridad en contenedores 343
Cloud Workload Protection 349

8. CLOUD 351

Introducción 351
Los conceptos a conocer 354
Nube pública 362
Riesgos 363

Amazon Web Services (AWS) 365
Microsoft Azure 375
Google Cloud Platform (GCP) 382
Estrategia de seguridad 385
Buenas prácticas de seguridad 386
Framework de controles y monitorización del cumplimiento 389
Protección de los datos en entornos SaaS 393

9. IDENTIDAD DIGITAL Y BIOMETRÍA 397

Futuro de la identidad digital 397
Introducción 398
Empoderando al individuo 399
¿Qué tecnologías determinarán el camino de nuestra identidad digital? 400
Identidad digital y Blockchain 401
Self Sovereign Identity 402
Aproximaciones privadas y gubernamentales 404
ESSIF 404
Alastria 406
Registro Cl@ve 406
Registros nacionales de identidades digitales 407
Identidad digital 408
Pero ¿qué es la identidad? ¿Y la identidad digital? 408
Ciclo de la identidad digital 410
Onboarding digital 412
Identity as a Service (IDaaS) 415
Proveedores de identidad 417
Autenticación 418
Métodos de autenticación 419
Ataques y técnicas a la identidad digital 427
Credencial Access TTP 427
Ataque a Kerberos: Golden Ticket 431
Biometría 438
Definición y origen 438
Modelos biométricos 439
Biometría comportamental o conductual 443

10. CRIPTOGRAFÍA Y BLOCKCHAIN 447

Introducción 447
Definición y tipos de sistemas criptográficos 448
Criptografía de clave simétrica 448
Sistemas clásicos 449
Sistemas modernos 450

Criptografía de clave pública 455
RSA 456
ElGamal 457
Algoritmos de Hash 458
MD5 459
SHA-1 460
SHA-2 460
SHA-3 461
Herramientas de análisis 461
La firma electrónica 463
Certificados digitales 464
Ámbitos de aplicación 470
Algunas aplicaciones y protocolos 472
SSL/TLS 472
IPSec 475
SSH 476
Firma electrónica de documentos 476
Beneficios de la firma electrónica 476
Firma electrónica vs. firma digital 478
Tipos de firma electrónica vs. legislación 478
Ataques y programas de análisis 479
Fuerza bruta distribuida 479
Tablas Rainbow 480
Cryptool 480
Aircrack-ng 480
John the Ripper 480
Cain & Abel 481
mitmproxy 482
sslstrip 482
Blockchain 482
Historia de Blockchain: Bitcoin 484
Ataques a la red de Bitcoin 485
Smart contracts 486
Ethereum 487
Características de las redes Blockchain 488
Algoritmos de consenso 489
Inmutabilidad 497
Como conclusión 497
Proyectos y redes de Blockchain 498
Hyperledger 498
Quorum 499
Ripple 500
Redes públicas y privadas 500
Blockchain públicas 500

Blockchain privadas 501
Blockchain híbridas 504
Trilema de la escalabilidad 505
Descentralización 506
Seguridad 506
Escalabilidad 507
Como conclusión 509
Retos de seguridad y amenazas de Blockchain 509
Amenazas 509
Ataques a la tecnología 512
Blockchain en la *dark web* 513
¿Qué es la *dark web*? 513
¿Cómo puede apoyar Blockchain a la *dark web*? 515
Ámbitos de aplicación 517
Un caso de uso apasionado que deberías conocer: diamantes de sangre 519

11. METODOLOGÍA DE *PENTESTING* **521**

Introducción 521
Metodologías 522
OWASP 523
OSSTMM 525
NIST SP800-115 525
Fases generales de un test de intrusión 526
Information Gathering: información pública 527
Reconocimiento del DNS 528
Google Hacking 533
Otras herramientas útiles para la búsqueda de información pública 540
Information Gathering: consulta activa 542
Enumeración de activos mediante DNS 543
Uso de ICMP 544
Escaneo de objetivos 545
Técnicas de enumeración 552
Análisis de vulnerabilidades 557
Clasificación y fuentes 557
Fabricantes 559
Herramientas 561
Trabajar con *exploits* 563
Metasploit 564
Componentes de Metasploit 565
Exploits 570
Uso de Metasploit 571
Explotación manual 574
EternalBlue 575

Escalado de privilegios....582
Vulnerabilidades en el sistema operativo....583
Escalado con Meterpreter....587
Ataques a credenciales....590
Credenciales comprometidas....591
Ataques....592
Gestión de las credenciales en Linux....595
Robando credenciales en Linux....599
Gestión de credenciales en Windows....602
Robando credenciales en Windows....608
Credenciales en equipos de red....614
Captura de tráfico en la red....614
Wireshark....615
Finalizando una intrusión....619
Eliminar las evidencias de un ataque....619
Trabajo en equipo....620
Diferencias y definiciones....621
Misiones basadas en inteligencia de amenazas....624

12. EXPLOITING 627

Introducción....627
Pila....628
Registros....628
Instrucciones de ensamblador....629
Buffer overflow....630
Fuzzing....633
Controlar el registro EIP....636
Bad characters....641
Búsqueda de direcciones de retorno y ejecución de código....642
Backdoors en aplicaciones portables....646
Demostración de inserción de código manual....647
Uso de herramientas automáticas....654

13. DATA EXFILTRATION 657

Introducción....657
Casuísticas....658
Estadísticas y casos actuales....660
Clasificación de la información....662
Técnicas y tácticas de ataque....664
Fugas en herramientas colaborativas....670
Controles de protección del dato....671
Protección de datos almacenados....672
Protección de datos en movimiento....672

14. ANÁLISIS FORENSE 675

Introducción 675
Ciencia e informática forense 675
Principios de la informática forense 677
Principio de transferencia de Locard 677
Borrado parcial de información en los dispositivos de almacenamiento electrónico ... 678
Memoria virtual y archivos temporales 679
Guías y definiciones 680
La evidencia digital 681
Ciclo de vida para la administración de la evidencia digital 681
Tipos de análisis forense y dispositivos 684
Discos duros 685
Motivos de un análisis forense 686
Uso particular o negocio 686
Legal y cibercrimen 687
Etapas de una investigación forense 688
Estudio 688
Adquisición 688
Análisis 689
Presentación 689
CSIRT 690
Incidente 690
Análisis forense en un CSIRT 691
CSIRT españoles 691
Herramientas forenses 692
Clasificación de herramientas 693
Herramientas de análisis 711
Análisis sencillo sobre Windows 714
Motivo del análisis 715
Información del sistema operativo 715
Información de red 720
Información de tareas, aplicaciones, componentes, servicios y otros 720
Información sobre *malware* 726
Información acerca de la actividad del usuario 728
Información acerca de los ficheros temporales 729
Información acerca del historial de navegación 730
Retos del forense en entornos *cloud* 735

ÍNDICE ALFABÉTICO 736



Introducción

Nuevas tecnologías, nuevos retos

Vivimos rodeados de tecnología, vayamos donde vayamos y hagamos lo que hagamos, siempre nos apoyamos en ella. Cada vez más, a veces sin darnos cuenta, utilizamos nuestros *smartphones*, o incluso *wearables*, para realizar todo tipo de transacciones y procesos de nuestro día a día. Volcamos todo tipo de información de nuestra vida, nuestras aficiones y nuestros gustos, y nos comunicamos con todo tipo de personas, a través de las redes sociales. Buscamos todo tipo de información y compramos muchos productos a través de la gran cantidad de portales donde se vende casi de todo sin tener que movernos de nuestra casa. Toda esta información que movemos desde nuestro teléfono de última generación, *tablet* u ordenador personal podría estar comprometida y sería accesible a un intruso malintencionado si no tomamos las medidas oportunas.

No es raro leer en los medios de comunicación noticias que tratan de identidades suplantadas y datos robados a través de Internet. Los usuarios debemos concienciarnos (y concienciar) de lo vulnerables que podemos llegar a ser cuando no controlamos ni conocemos la manera en la que los datos se están moviendo y almacenando en la red, acrecentándose este desconcierto con la famosa nube o *cloud*.

Nunca le daría su número de cuenta bancaria o su tarjeta de crédito a otra persona, pero ¿qué pasa si las escribo en una página web donde voy a realizar una compra? Muchas veces confiamos en portales de venta de productos, simplemente porque vemos logotipos de empresas certificadoras o de verificación de calidad, pero ¿podrían estar engañándonos? ¿Podría no tratarse de esa empresa que dice ser?

Y esto no es un problema que tengamos únicamente en el ámbito personal; en el ámbito profesional, donde el objetivo de los cibercriminales es mucho mayor y el impacto puede ser terrible, las personas seguimos siendo el eslabón más débil de la cadena. No importa si nuestra empresa se gasta millones de euros en adquirir tecnología avanzada de protección del perímetro, protección del puesto de usuario, medidas *antiransomware* y tecnologías disruptivas (*web isolation*, *cloud workload protection*, etc.), los usuarios de los recursos tecnológicos de nuestra compañía debemos ser cautelosos frente a todas las amenazas que se nos presentan, ya que vamos a ser los objetivos de los atacantes para conseguir una vía de entrada a la información y sistemas de una organización.

El ciberespacio es un mundo ideal donde podemos hacer casi cualquier cosa sin salir de nuestra casa, pero es tanta y tan variada la información que movemos a través de la red, que es lógico pensar que será muy cotizada por todo tipo de usuarios malintencionados. Por ello, debemos conocer muy bien cómo funcionan los distintos portales de Internet y con qué medidas de protección contamos para poder hacer uso de la tecnología, sin que ello nos provoque un problema de privacidad o seguridad de nuestra información.

A través de este libro le presentaremos la ciberseguridad y las nuevas tecnologías, poniendo al descubierto sus debilidades y enseñándole a protegerse de ellas. Veremos cómo hacer los sistemas más seguros y que sea capaz de utilizar todo tipo de herramientas y servicios en la red, sabiendo que la privacidad de su información y sus datos se encuentran totalmente seguros.

Objetivos del libro

Nos encontramos ante un libro técnico que, de manera clara y concisa, nos enumera las diferentes técnicas y herramientas de seguridad y ciberataques disponibles sobre las más actuales tecnologías.

Creemos fundamental que el usuario se sienta confortable cuando navegue por Internet y que domine los conceptos básicos de ciberseguridad y privacidad de la información. Por ello, lo que pretendemos es que, tras la lectura de este libro, tenga claro las amenazas y vulnerabilidades de los sistemas de información y pueda tomar las medidas oportunas para protegerse de ellas.

Podemos decir que con estas páginas despertaremos un deseo por conocer y aprender mucho más de los sistemas, así como las ganas de estar al día y seguir formándose en el mundo de la ciberseguridad, pues este entorno es como un ser vivo, evoluciona día a día con nuevas herramientas y servicios.

Organización del libro

Hemos dividido el libro en capítulos, que tratarán todos los temas actuales en cuanto a ciberseguridad y *hacking* se refiere, pasando por muchas de las últimas tecnologías y herramientas. En cada uno de los temas utilizaremos las herramientas o aplicaciones necesarias para ayudar al lector, mediante ejemplos, a entender las diferentes vulnerabilidades y su explotación o de qué forma se puede proteger correctamente una infraestructura. Todas las herramientas utilizadas en el libro tienen sus licencias, unas serán con licencia gratuita y otras de pago, por lo que el lector deberá descargarlas de los sitios oficiales de cada una de ellas si desea utilizarlas.

A continuación, enumeramos los diferentes temas sobre los que tratará este libro:

1. **El mundo digital es inseguro:** Este primer capítulo servirá de introducción e iniciación, y nos hará descubrir el por qué necesitamos conocer a fondo los sistemas y las aplicaciones que utilizamos antes de interactuar libremente en el ciberespacio. También analizaremos las últimas cifras del ciberespacio, lo que nos dará una idea de la superficie de ataque de los tipos malos.
2. **Ciberamenazas:** En este capítulo veremos las principales ciberamenazas a las que nos enfrentamos, cuál es el *modus operandi* de los tipos malos, cómo están evolucionando estas amenazas, qué tipos existen, qué actores suelen utilizarlas, ataques famosos relacionados con cada una de ellas y cómo protegernos.
3. **Ciberguerra:** En este capítulo hablaremos de ciberguerra y ciberespionaje. Veremos la historia de la ciberguerra, principales ataques y finalmente, analizaremos los *targeted attacks* y *advanced persistent threats.*
4. ***Hacker Mindset*:** Este es un capítulo totalmente nuevo en esta edición. Hemos querido analizar desde un punto de vista psicológico cuál es la psicología del cibercriminal, cuáles son sus motivaciones. También analizaremos los perfiles criminales desde los tiempos de la Unidad de Ciencias del Comportamiento del FBI hasta nuestros tiempos. Veremos las técnicas de persuasión que utilizan los ciberatacantes y, finalmente, iremos viendo cada unos de los tipos de *threat actors*, cuáles son sus motivaciones, los tipos de ataques que ejecutan habitualmente y los ataques conocidos para cada uno de ellos.
5. **Arquitecturas de red y datos: defensa y ofensiva:** En este capítulo se presentará tanto la defensa de la red como diferentes técnicas de ataque a protocolos de comunicaciones. Repasaremos los conceptos básicos en los que se apoya cualquier red de datos, explicando cada una de las capas de red y los protocolos utilizados. También daremos un pequeño repaso a la arquitectura de sistemas de seguridad e introduciremos los diferentes elementos de seguridad con los que contamos. Además, se mostrará al usuario cómo funcionan las redes *wireless* y VoIP, enumerando algunos de sus ataques y viendo cómo podremos protegernos ante ellos.

6. **Mundo Industrial e IoT:** En este capítulo se realizará una introducción a las tecnologías convergentes presentes en los entornos industriales y se expondrán las vulnerabilidades y posibles ataques que los sistemas SCADA pueden sufrir. Por último, se expondrán unas breves ideas sobre la seguridad en el Internet de las Cosas.
7. ***Hacking web* y seguridad en microservicios:** En este capítulo se presentarán las vulnerabilidades web más conocidas y se realizarán ejercicios prácticos para entenderlas. También se hará una introducción a los microservicios y a las tecnologías de contenedores, presentando su modelo de seguridad y sus posibles vulnerabilidades.
8. ***Cloud*:** En este capítulo se da una visión muy completa de todos los aspectos de seguridad a tener en cuenta con respecto al uso de la nube pública. Se analizarán los proveedores principales para destacar aquellas soluciones nativas de seguridad que ofrecen como parte de su producto, y se ofrecerá un conjunto de buenas prácticas para que el lector pueda entender cómo proteger estos entornos.
9. **Identidad digital y biometría:** En este capítulo abordaremos la identidad digital, el futuro de la misma, la identidad digital soberana, *onboarding* digital, IDaaS, autenticación, tácticas técnicas y procedimientos de MITRE y ejemplos prácticos de ataques.
10. **Criptografía y Blockchain:** Se hará un repaso de todos los conceptos de criptografía relevantes. Veremos cómo funciona *Blockchain* y qué riesgos puede tener su uso, así como las mejores prácticas para construir una cadena de bloques segura.
11. **Metodología de *pentesting*:** En este capítulo pondremos los sistemas al descubierto, mostrando cómo someter a los mismos a ciertas pruebas de intrusión, para detectar sus vulnerabilidades, llevando a cabo una metodología de test de intrusión de principio a fin. Evaluaremos las mejores herramientas para llevar a cabo este tipo de pruebas.
12. ***Exploiting*:** En este capítulo se hará una introducción al mundo del análisis y creación de *exploits*. Se presentarán conceptos, técnicas y herramientas que permitirán al lector realizar pequeñas pruebas con las que entender el funcionamiento de códigos que consiguen explotar vulnerabilidades reales.
13. **Data Exfiltration:** En este capítulo se realizará una revisión de todas las técnicas, tácticas y procedimientos que pueden llevar a sufrir brechas de seguridad que afecten a la información, es decir, fugas de información. Se presentarán estadísticas y conceptos para poder entender cómo construir un modelo de protección *data driven* en una compañía.
14. **Análisis forense:** En este capítulo nos adentraremos en este apasionante mundo de la informática forense. Veremos de qué trata, cómo actúa y las herramientas más utilizadas en este campo.



1 El mundo digital es inseguro

Tiempos de incertidumbre

Es increíble echar la vista atrás y recordar cómo eran las comunicaciones hace tan solo 30 o 40 años. No existía Internet, ni por supuesto los teléfonos móviles, ni nada que se le pareciera. Teníamos un teléfono fijo por cada casa y esa era la manera de comunicarnos con nuestros seres queridos. Es más, desde que se inventó el teléfono en el siglo XIX, este ha tenido una evolución imparable. Ha pasado de ser un objeto de lujo a ser algo indispensable en nuestras vidas. Si pensamos en los tiempos de nuestros abuelos, ni siquiera había un teléfono para llamar desde tu propia casa, sino que lo que existía era un teléfono público para todo el pueblo. Había que acercarse al teléfono del pueblo, que podía estar en una cabina o en la casa de un particular, hacer cola, llamar y, al otro lado del teléfono, tenía que estar la persona que buscabas esperándote en el teléfono de su pueblo para responderte, algo impensable hoy en día.

Fue en la década de los setenta cuando el teléfono dejó de ser un artículo de lujo para generalizarse su instalación en las casas ¿Os imagináis la vida hoy en día así? Creo que nos costaría adaptarnos, quién sabe, quizás algún día acabamos enviando mensajes mediante cuervos, como en nuestra querida serie *Juego de tronos*, sería todo un reto para nosotros.

El mundo, tal y como lo conocíamos, ha cambiado radicalmente en las últimas décadas de manera vertiginosa. Vivimos en un planeta hiperconectado, ya no solo por Internet o los dispositivos móviles, sino con otro tipo de dispositivos y, cada día, hay más de estos conectados a Internet, desde bombillas a neveras, coches o hasta ciudades enteras. Si pensamos en las tareas que llevamos a cabo a lo largo del día, es difícil que cualquiera de estas no esté

relacionada con un sistema informático. Realizamos todo tipo de actividades en la red, como pagos por Internet, consultar nuestras redes sociales o correo electrónico, realizar cursos *online*, teletrabajar, videoconferencias, etc. Casi cualquier tipo de actividad que pensemos, podemos llevarla a cabo a través de Internet en la actualidad. El problema que nos encontramos con todo esto es que permitimos a nuestros dispositivos almacenar y descargar abundante y valiosa información acerca de nuestra identidad y hábitos, como, por ejemplo, datos personales, rutinas diarias, geolocalización, gustos, etc. Es entonces cuando surgen dudas referentes a la seguridad de la información. ¿Estos datos se almacenan y viajan de manera segura? ¿Qué tipo de vulnerabilidades poseen los sistemas operativos y las aplicaciones que utilizamos? ¿Qué pasos tenemos que tomar para explotar estas vulnerabilidades sin ser detectados?



FIGURA 1.1. Teléfonos del siglo XIX.

Además, a todo este escenario complejo de comunicaciones, se suma la pandemia mundial derivada del nuevo coronavirus (SARS-CoV-2), una gran impulsora de la transformación digital en el mundo, lo que trae grandes beneficios, pero también grandes riesgos de ciberseguridad. Hemos pasado de trabajar todos los días en la oficina al extremo opuesto en poco tiempo, a trabajar desde casa o a un modelo mixto. Trabajar desde casa a partir de entonces se ha normalizado. Era algo a lo que inevitablemente íbamos a llegar en la mayoría de trabajos "digitalizados" con el paso del tiempo, dado que cada vez era más y más demandado por la sociedad, pero sin duda la pandemia lo precipitó. La proliferación del trabajo desde casa ha

traído consigo nuevos retos de ciberseguridad. Un ejemplo de ello es la industria de la salud, que fue una de las más atacadas en el pasado 2020; en esta industria, cuando se sufre un ciberataque, ya no hablamos de pérdidas monetarias o reputacionales, sino que hablamos de posibles pérdidas de vidas de personas, lo que es mucho más grave que los habituales ataques que solemos ver. Ya en 2020 veíamos uno de los primeros casos en el que por culpa de un ciberataque una persona fallecía en Alemania. Fue en el Hospital Universitario de Dusseldorf a costa de un *ransomware* que colapsó el servicio de urgencias el 18 de septiembre de 2020, afectando a 30 de sus servidores y teniendo que cerrar temporalmente la sala de urgencias.



ALEMANIA

Muere una mujer después de un ataque informático a un hospital de Dusseldorf que no pudo atenderla

La paciente, que estaba gravemente enferma, tuvo que ser trasladada a otro hospital y murió.

Vista en detalle de un teclado de ordenador. FRED TANNEAU AFP

FIGURA 1.2. Titular de la noticia sobre el fallecimiento de una paciente a raíz de un ataque de *ransomware* en el Hospital Universitario de Dusseldorf. Fuente *El Mundo*.

El perímetro de los sistemas de las empresas, tal y como lo conocíamos, se está difuminando. Si ya lo había hecho con el *cloud*, ahora aún más con los dispositivos conectados desde cualquier parte del mundo y con dispositivos personales en muchos casos. Las empresas ya no disponen de su perímetro seguro para proteger sus sistemas, lo que facilita la tarea a los

tipos malos, dado que disponen de muchos más puntos de entrada que encontrar para colarse en las redes de las compañías o particulares, desde dispositivos móviles personales, redes familiares en las casas de los trabajadores, sistemas en el *cloud*, dispositivos IoT, etc. Es por ello que la arquitectura tecnológica de las empresas (y, por tanto, la arquitectura de seguridad) se está replanteando en nuevos modelos centrados en el acceso desde cualquier parte y desde cualquier dispositivo como, por ejemplo, con las arquitecturas **SASE (Secure Access Service Edge)** y **Zero-Trust Network Access**, arquitecturas que veremos más adelante en el libro.

Además, cada vez más las compañías tienen más dependencias de terceros, por lo que los atacantes también pueden buscar posibles vulnerabilidades en estos, ya que almacenan datos y disponen de acceso a las redes de las empresas sobre las que dan servicios. Este tipo de ataques a empresas terceras es lo que se conoce como *supply chain attack,* ataque a la cadena de suministro, el cual veremos más en detalle en el próximo capítulo. Ejemplo de ello fue el ataque que sufrió British Airways a su pasarela de pagos. El código de la misma fue modificado entre el 21 de agosto y el 5 de septiembre de 2018, interceptando los pagos con tarjetas y pudieron robar así los atacantes valiosa información como nombre, apellidos, direcciones físicas, correo electrónico, números de tarjeta, fechas de expiración y códigos de seguridad de las mismas. Un total de 500.000 potenciales clientes afectados según el ICO y una multa de 205 millones.

También vimos durante el pasado 2020 un incremento en los ataques de *phishing*. Experimentaron un cambio de imagen a raíz de la pandemia y se volvieron más sofisticados, apuntando a plataformas y soporte técnico de aplicaciones como Skype, Zoom, Google Meet o Microsoft Teams. La amenaza fue tan elevada que el propio Grupo de Análisis de Amenazas de Google bloqueó 18 millones de correos por día de *phishing* y *malware* con temática COVID-19 en abril de 2020, como se puede ver en su propio blog en el artículo "Protecting businesses against cyber threats during COVID-19 and beyond", `https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond`.

Y pensarás: ¿no tenemos suficiente lidiando con la incertidumbre, el miedo y la confusión de estos tiempos? Los tipos malos no descansan, y necesitamos conocer sus técnicas y estrategias para luchar contra ellos. Para eso, os hemos traído este libro, donde analizamos en detalle estas técnicas y estrategias de ataque y las motivaciones que les atañen.

Grandes cifras

Si nos remitimos a los datos, en el informe *Digital 2020. Global Digital Overview* realizado por We Are Social (`http://www.wearesocial.sg/`), podemos ver un gran número de estadísticas referentes a indicadores sociales. El informe deja claro que el mundo digital, dispositivos móviles y redes sociales se han convertido parte indispensable de nuestras vidas.

Como datos generales, si en el mundo somos un total de 7.800 millones de personas, sorprendentemente tenemos un total de 4.500 millones de personas en el mundo que utilizan Internet, el 60 % de la población mundial está conectada. Las redes sociales han pasado la marca de los 3.800 millones, más de la mitad de la población mundial utiliza las redes sociales.

No obstante, estos datos todavía presentan grandes retos. La mayoría de usuarios conectados a Internet viven en economías desarrolladas, el 40 % de la población mundial no está conectada a Internet, siendo las mujeres, según los datos, las que tienen menos probabilidad de estar conectadas y, en lugares como en Asia del Sur, vemos una brecha de género considerable donde la cifra de hombres que utilizan las redes sociales es tres veces mayor que la de las mujeres.

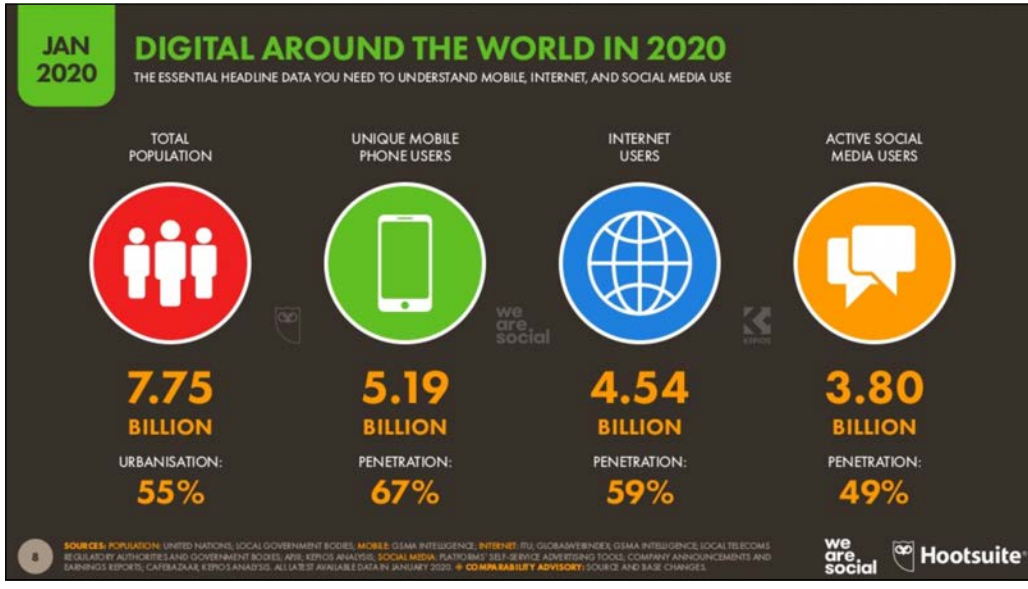


FIGURA 1.3. Global Digital Snapshot. We are social.

Otro dato interesante es el del tiempo de uso. Si permanecemos viendo la televisión de media 3 horas al día, en Internet lo hacemos de media 7 horas al día, es decir, más del 40 % de nuestro tiempo del día, y su uso en dispositivos móviles supone más de la mitad de dicho tiempo de uso. Cinco mil millones de usuarios únicos en movilidad. Respecto a las cifras de uso de Internet, el total de usuarios de Internet es de más de tres millones y medio de personas, es decir, un 50 % de la población total mundial y un total de casi 3 millones de personas de usuarios activos en redes sociales, es decir, un 74 % de los usuarios que hacen uso de Internet también lo hacen de las redes sociales.

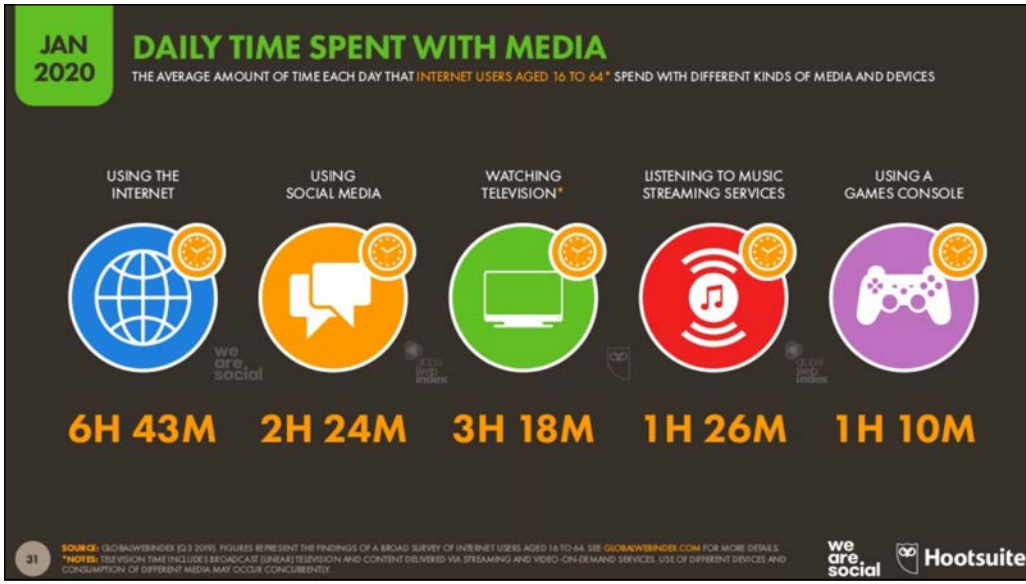


FIGURA 1.4. Daily Time Spent with Media. We are social.

Otra de las estadísticas interesantes es el crecimiento del último año (de enero de 2019 a enero de 2020). Si la población mundial creció un 1,1 %, el número de usuario móviles creció un 2,4 %, el número de usuarios de Internet un 7 %, y el número de usuarios activos en redes sociales un 9,2 %.

También podemos ver, en estas estadísticas, el alcance de Internet por regiones, donde América del Norte y Europa se llevan la palma al superar con creces el resto de regiones. África y Asia reflejan los menores índices de penetración de Internet con un 34 % y un 56 %. De hecho, las regiones con menor índice son, con 22 %, África Central y, con un 23 %, África del Este.

Cuando veíamos estas estadísticas proporcionadas por We Are Social en el informe del 2014 en nuestras anteriores ediciones, el alcance de Asia Sur y África era de un 12 % y 18 % respectivamente. En la última edición, con datos del 2017, el alcance era de un 33 % y un 29 % respectivamente. Por lo que es sorprendente cómo, en pocos años, va llegando de manera global Internet a todas las regiones.

Veamos datos interesantes por país. Si observamos el crecimiento en Internet por países, algunos países como Congo, República Democrática del Congo o Samoa son los que han visto el mayor crecimiento. En Corea del Norte, Internet continúa bloqueado. Y en los siguientes países son los que presentan mayor porcentaje de entrada: Islandia, Catar, Emiratos Árabes Unidos y Baréin.

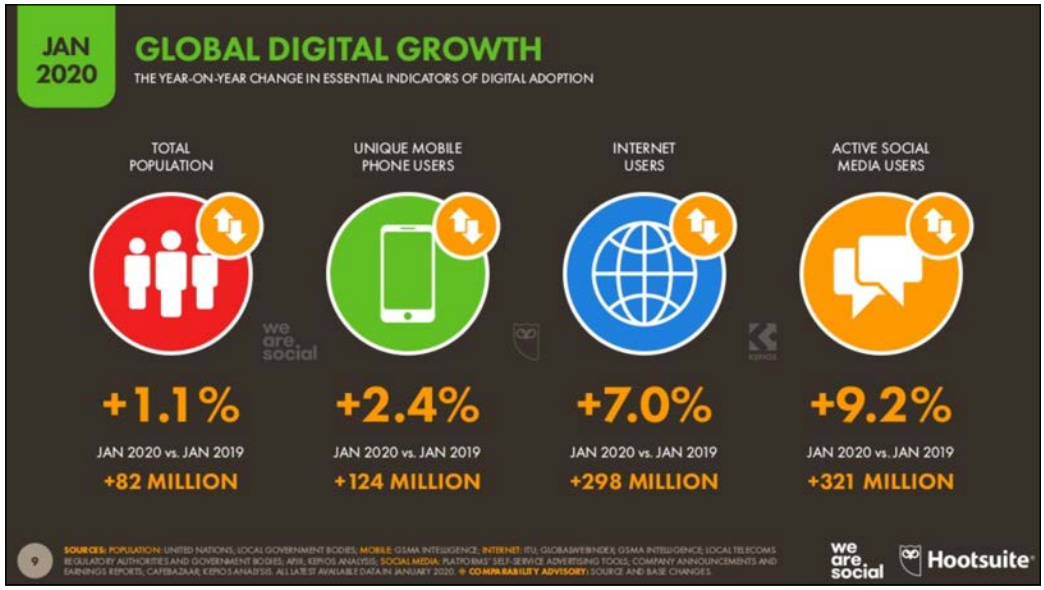


FIGURA 1.5. Global Digital Growth. We are social.

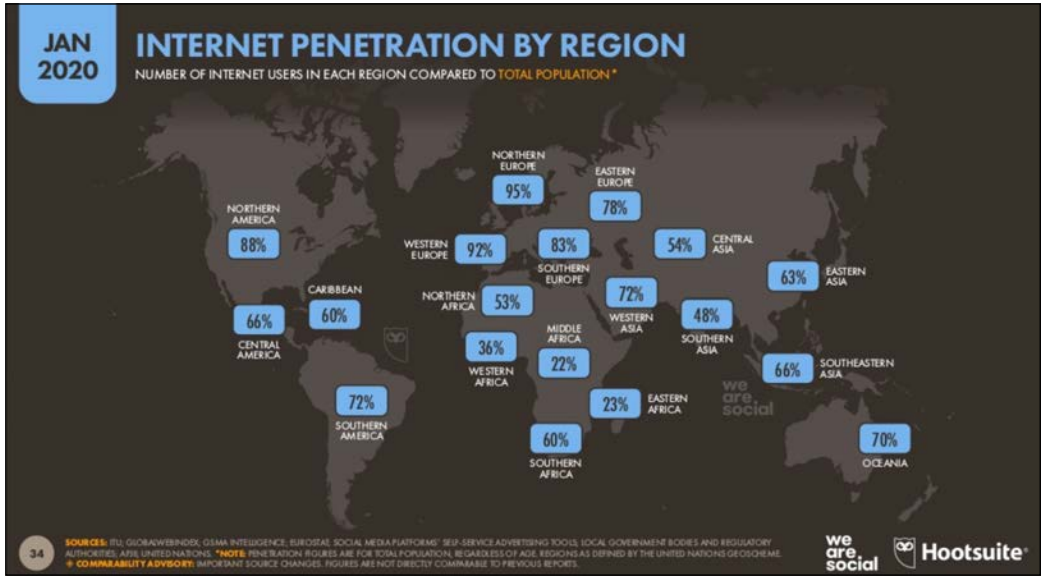


FIGURA 1.6. Internet Penetration by Region. We are social.

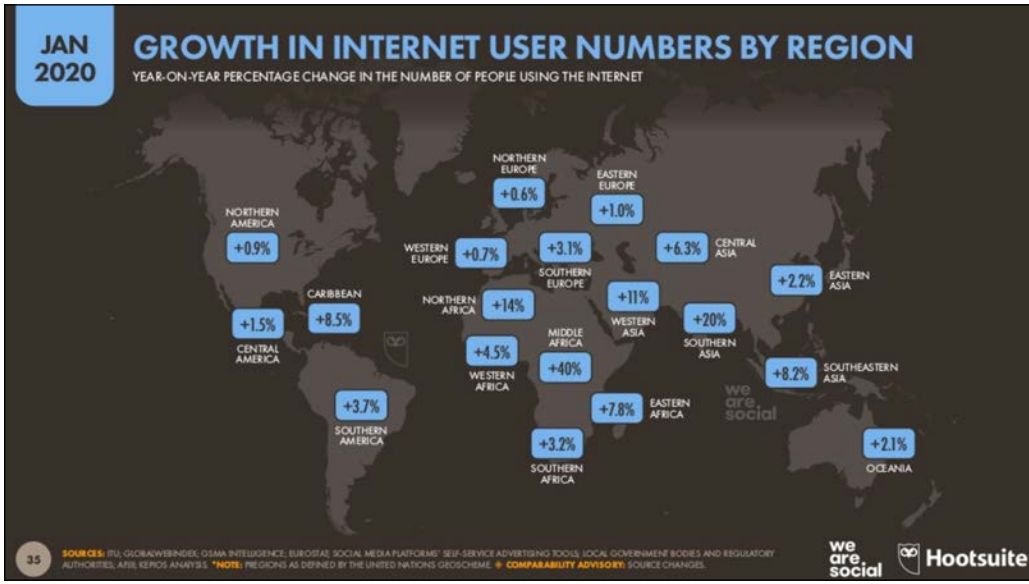


FIGURA 1.7. Growth in Internet User Numbers by Region. We are social.

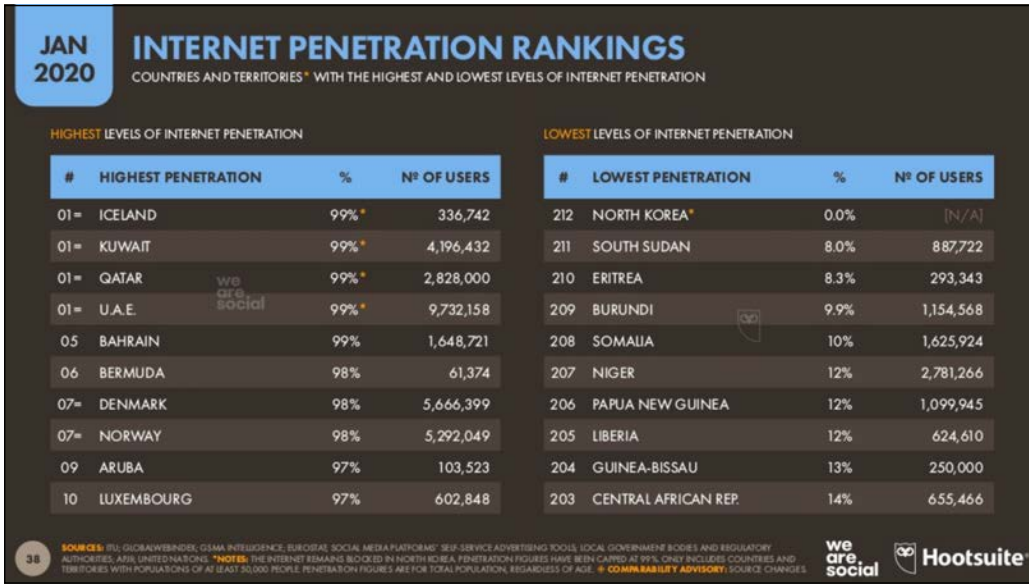


FIGURA 1.8. Internet Penetration Rankings. We are social.



FIGURA 1.9. Internet Growth Rankings: Relative Change. We are social.

Por último, en el caso de las redes sociales, resulta interesante ver el número de usuarios activos diariamente frente al total de usuarios. Podemos ver cómo en España estamos por encima (62 %) de la media mundial (49 %) y que, sorprendentemente, en países tan dispares como India y Nigeria la media es muy inferior. También resulta interesante ver los datos concretos por países, por ejemplo, el caso de España. La población total es de 46,75 millones de personas, existen más dispositivos móviles que personas, un 116 %. El uso de Internet supone un 91 % de entrada y el total de usuarios en redes sociales supone un 62 %.

Estos datos son muy interesantes para valorar a nivel mundial, y concretamente por países, cómo está evolucionando el entorno social digital, así que invitamos a nuestros lectores a que naveguen por la web de We Are Social, que ofrece un gran número de estudios estadísticos de mucho valor: `https://wearesocial.com/digital-2020`.

Veamos ahora cómo pueden evolucionar estos datos en el futuro para tratar de anticiparnos a lo que nos espera. Si nos remitimos al informe *Cisco Annual Internet Report (2018–2023) White Paper*, podemos analizar algunas estimaciones interesantes del uso de nuevas tecnologías. Vemos que dos tercios de la población mundial tendrá acceso a Internet en 2023, un 66 % de la población mundial respecto a un 51 % de 2018. Respecto a los dispositivos conectados a redes IP, habrá el triple que población mundial en 2023, lo que suponen 3,6 dispositivos en red por persona o 29.300 millones de dispositivos. Y, respecto a los dispositivos móviles, más del 70 % de la población mundial tendrá acceso a Internet a través de dispositivos móviles en 2023, un 71 % en 2023 frente a un 66 % que había en 2018.

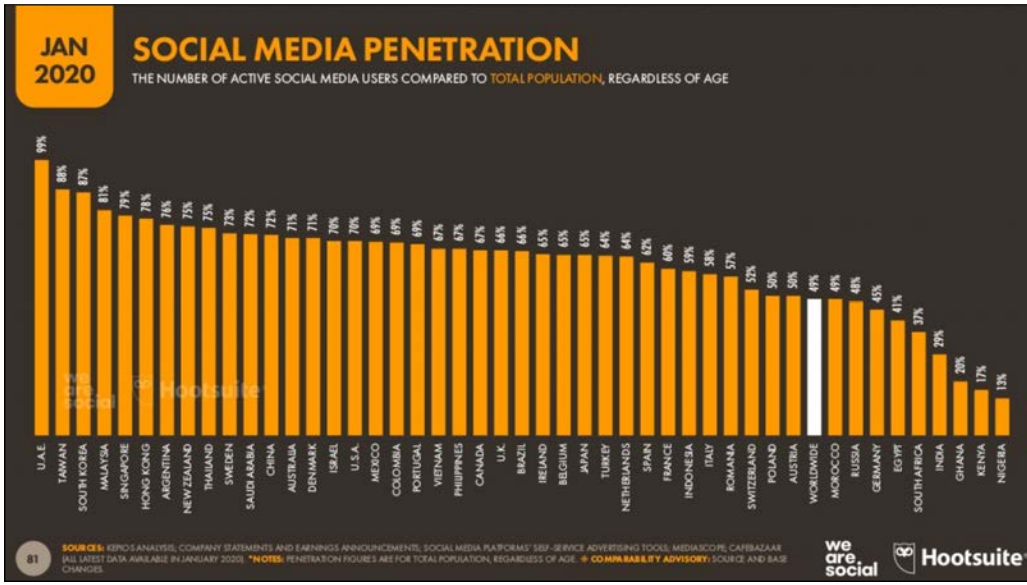


FIGURA 1.10. Social Media Penetration. We are social.

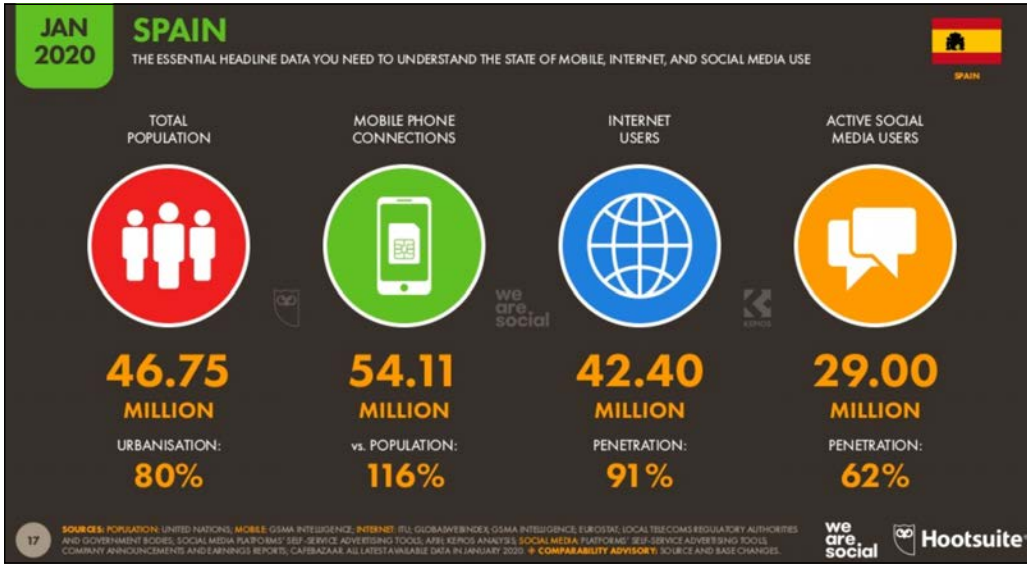


FIGURA 1.11. Spain. We are social.



FIGURA 1.12. Global Mobile Device and Connection Growth.

Es fascinante observar cómo cada vez existen más conexiones a Internet, se incrementa el uso de dispositivos móviles, de dispositivos IoT o el consumo redes sociales y cómo cada vez la velocidad de conexión es más rápida, el 5G ya está aquí entre nosotros. ¿Llegará un día en que absolutamente todo el planeta tenga conexión a Internet? ¿Llegará el día en que todos los trámites se realicen a través de Internet sin movernos de nuestra casa? Lo que está claro es que Internet es una *commodity* en, prácticamente, todo el mundo y que hemos llegado al punto de no poder vivir sin él, tanto a nivel particular como a nivel empresarial.

Pero esto nos lleva al problema de que los ataques y el fraude son cada vez más digitales, mezclando riesgos tecnológicos con riesgos en el proceso, ya que no todos los ciberataques son resultado de explotar una vulnerabilidad. La debilidad en la implementación de un proceso tecnológico puede ser el causante de un fraude con resultados de pérdidas económicas. Con tan solo unos pocos recursos, los tipos malos son capaces de robar millones de euros, mucho más sencillo. Lo que también es cierto es que las empresas están cada vez más protegidas, así que afortunadamente cada día se lo ponemos un poco más difícil a los tipos malos, pero no nos podemos dormir, porque las técnicas de ataque van evolucionando como lo hacen las tecnologías y cada vez son más ingeniosas, así que los profesionales de la ciberseguridad debemos de estar actualizados y mantenernos al pie del cañón día a día.

Filosofía *hacker* y argot

Probablemente hayamos escuchado el término "*hacker*" en multitud de noticias y películas refiriéndose a un tipo con propósitos maliciosos que entra en los sistemas para robar información o simplemente "atacarlos" sin más.

Algunos de los filmes más conocidos que muestran esta imagen del hacker son *La Red* (1995), *La Jungla 4.0* (2007), *Hackers* (1995), *Operación Swordfish* (2001), *23. Nada es lo que parece* (1998), *Firewall* (2006), *Blackhat: amenaza en la red* (2015) y *Juegos de guerra* (1983) y series destacadas como *Mr. Robot* (2015). Cabe destacar que en una película tan futurística como *Matrix Revolutions* (2003) se muestra una imagen más cercana a la realidad que en otras muchas, ya que, en una de las escenas, Trinity realiza un ataque SCADA a una central eléctrica, haciendo uso de la herramienta Nmap para el escaneo de puertos y explotando una vulnerabilidad a continuación en el servidor SSH, vulnerabilidades descubiertas en el 2001. En otras películas como en *The Listening* (2006) o *Battle Royale* (1999) se puede ver también parte del código de Nmap.



FIGURA 1.13. El mundo *hacker* es un tema recurrente en la literatura y en el cine.

Dejando a un lado los motivos y estudiando las técnicas que utilizan, el *hacking* es una metodología poco ortodoxa que se basa en resolver problemas. La mentalidad que desarrollan los *hackers* es una mentalidad completamente analítica, con determinados *skills*: análisis de información, resolución de problemas y toma de decisiones. Estas fortalezas les permiten incrementar su probabilidad de éxito y productividad a la hora de enfrentarse a los retos. Además, requiere de cierta creatividad para detectar vulnerabilidades y fallos de seguridad en los datos, programas, infraestructuras, etc. A menudo los *hackers* deben de tener un pensamiento *out of the box* para encontrar las soluciones. ¡Te animamos a que te enfrentes a algún reto *hacking* tipo *capture the flag* o *hackaton*, para que lo experimentes en primera persona! Algunos sitios web para practicar CTF son CTF365, OverTheWire o Hacking-Lab. Te recomendamos que visites esta página web si quieres descubrir más: `https://www.quora.com/What-are-the-best-online-hacking-and-CTF-websites`.



FIGURA 1.14. CTF365. Security Training Platform.

El término "*hacker*" se comenzó a gestar en los años 60 gracias a las computadoras del MIT (Massachusetts Institute of Technology) como alguien que es experto con los ordenadores, con muy buenas habilidades de programación y que hace uso de estas habilidades para ganar conocimiento junto a otros. Un *hacker* en origen no entra en sistemas ajenos con propósito malicioso o para beneficio personal. Debido a esta confusión mediática, la palabra *hacker* se ha ido desvirtuando, y es por lo que ha ido surgiendo la diferenciación entre *white hats*, *grey hats* y *black hats*, así como la creación de otras clasificaciones o tipologías como son los *insiders, script kiddies o phreakers*.

White hat, *sneaker* o hacker ético

White hat o ***hacker* de sombrero blanco** son términos que entran dentro de la definición original de *hacker* y, en ocasiones, se les llama ***hackers* éticos** o ***sneakers***. Estos términos se refieren a un *hacker* o experto en seguridad informática que está especializado en realizar test de intrusión o evaluaciones de seguridad, con ánimo de garantizar la seguridad de la información de los sistemas de una empresa. El término fue acuñado en origen por IBM. Algunos de los *hackers* éticos trabajan en equipos llamados ***red teams*** o ***tiger teams***.

Bug bounty o programas de recompensa

Una de las prácticas más generalizadas en los últimos años por este tipo de *hackers* ha sido el participar en programas de recompensa, más conocidos como ***bug bounty***. Si habitualmente las empresas contratan a profesionales para que realicen *penetration testing* a las aplicaciones o sistemas, existen determinadas plataformas, como HackerOne o BugCrowd entre otras, que permiten a las empresas interesadas auditar sus servicios de ciberseguridad conectando a *hackers* éticos de todo el planeta, dispuestos a atacar los servicios de estas compañías a cambio de una sustancial recompensa económica. Cualquiera puede inscribirse y participar en estos programas de *bug bounty*. También hay empresas tecnológicas que directamente anuncian recompensas para todos aquellos que reporten vulnerabilidades, incluso existen "muros de la fama", donde estas empresas reconocen a estas personas poniendo su nombre o *nickname* y el código CVE de la vulnerabilidad reportada.

Black hats o *crackers*

Los ***black hats*** o ***crackers*** son el opuesto a los *hackers*. Se tratan de expertos en ordenadores y con buenas habilidades para atacar sistemas, por lo que estos entran en los sistemas con propósito malicioso o para beneficio personal. Los ***hackers* de sombrero negro**, una vez que ganan acceso a estos sistemas, tienen como objetivo causar algún tipo de daño al sistema, como, por ejemplo, robo de información, borrar ficheros, cortar el acceso a sistemas o modificar sitios web. Los *black hats* pueden ser desde personas que irrumpen en sistemas por "amor al arte", hasta grandes mafias organizadas para cometer fraudes graves. En el capítulo 3, ampliamos estos perfiles del atacante, técnicas y psicología de los mismos.

Grey hats

Grey hats o ***hackers* de sombrero gris** son *hackers* que en ocasiones respetan las leyes y en otras actúan de manera ilegal. Son una mezcla entre *black* y *white hats*. Normalmente no atacan malintencionadamente o con intereses personales, pero tienen el conocimiento suficiente para cometer delitos. Si los *white hats* normalmente avisan a las empresas de las brechas de seguridad que han encontrado, los *grey hats* normalmente hacen alerta de estas vulnerabilidades en la comunidad *hacker*. Sus motivaciones pueden ser múltiples, como el ánimo de lucro, protestas o desafíos personales. La forma de protesta puede estar ligada al hacktivismo, donde se hace uso de técnicas maliciosas con ánimo de difundir un mensaje político o ideológico, del que hablaremos más adelante en relación con la ciberseguridad.

Insiders

Se trata de personas que trabajan dentro de una organización, como empleados o externos que disponen de acceso a los sistemas. Debido a la cantidad de información que tienen los ***insiders*** acerca de los sistemas, aplicaciones, procesos y empleados de la empresa y a las

habilidades que poseen, pueden causar grandes daños y repercutir en pérdidas monetarias significativas. Normalmente, los ataques de este tipo de colectivo vienen motivados por despidos en el trabajo o porque se encuentran compinchados (o bajo coacción) con bandas organizadas.

La categoría de *insiders* se mueve dentro de un continuo entre realizar un acto malintencionado de mala fe, o bien llevar a cabo un acto negligente sin conocimiento de que se está produciendo una brecha de seguridad, incumpliendo las políticas internas de la organización.

Podemos identificar tres tipos de *insiders*:

- ***Malicious insiders*:** Personas que tratan de hacer daño a la organización para obtener un beneficio.
- ***Negligent insiders* o negligentes:** Son personas que cometen errores en la organización porque ignoran las políticas internas.
- ***Infiltrators* o infiltrados:** Se trata de actores externos que tratan de ganar acceso a la organización como personas legítimas para obtener información o causar daño.

Script kiddies

Se trata de un término despectivo para definir a un atacante inexperto que es capaz de ejecutar un *script* o una aplicación (desarrollados por otros) para llevar a cabo un ataque. Los ***script kiddies*** normalmente no tienen un alto nivel de programación o conocimiento de las aplicaciones que usan, por lo que, cuando sus ataques han concluido, dejan muchas huellas y se les puede rastrear con facilidad.

Phreakers

El ***phreacking*** se trata de un tipo de *hacking* que consiste en irrumpir en sistemas telefónicos. Para realizar este tipo de ataque se requiere un amplio conocimiento en telecomunicaciones y algunos de estos atacantes tienen experiencia trabajando en empresas de telefonía o negocio de telecomunicaciones. Un ejemplo de ataque es a sistemas PBX (*Private Branch Exchange*), que se trata de centrales telefónicas.

Conceptos y enfoques

Es importante conocer unos pocos conceptos básicos de seguridad para conocer mejor el entorno y el objetivo a atacar.

Conceptos básicos de seguridad: CIA

CIA se refiere a los tres pilares de la seguridad: confidencialidad, integridad y disponibilidad (*availability*, en inglés). Cuando pensamos en seguridad, debemos pensar en estos tres principios que nos llevan a las siguientes cuestiones: ¿se almacenan o viajan los datos de manera confidencial? ¿Se asegura la integridad de los datos? ¿Están los datos disponibles para los usuarios de la organización?

- **Confidencialidad:** Cuando hablamos de confidencialidad, nos referimos a las medidas que se necesitan tomar para evitar la revelación de la información a personal no autorizado. Recordemos que la información es considerada a día de hoy el activo más valioso en cualquier compañía (datos de usuario, patentes, procesos de negocio, etc.).

  Para los usuarios, la confidencialidad es muy importante, ya que si los datos de estos se ven revelados podría resultar en un robo de identidad, fraude o pérdidas monetarias. Para una organización podría ser todavía peor, ya que la pérdida de confidencialidad de ciertos datos de los usuarios estaría penada por el Reglamento General de Protección de Datos (RGPD) y podrían llegar a sufrir graves sanciones de hasta 20 millones de euros o el 4 % de la facturación global de la compañía, que vendrían impuestas por la Agencia Española de Protección de Datos. El nuevo Reglamento de Protección de Datos Europeo (RGPD), que vio la luz en 2018, ha tomado una importancia clave para velar por la privacidad y derechos de los clientes respecto a cómo se gestionan, almacenan y eliminan los datos de estos.
- **Integridad:** Este término se refiere a los mecanismos y acciones tomadas para proteger la información almacenada, o en tránsito, de alteraciones no permitidas. Las medidas de integridad aseguran que los datos enviados llegan al receptor sin ningún tipo de alteración. Esto es posible, por ejemplo, mediante firmas digitales, utilizando algún programa como **OpenPGP** o compatibles con **S/MIME**, que cifran la información en origen y la descifran en destino solo si el destinatario está legitimado para ello.
- ***Availability*** o **disponibilidad:** Este término se refiere a que los usuarios puedan mantener las comunicaciones entre sistemas y acceso a los datos que sean necesarias. Los mecanismos para asegurar la disponibilidad pueden variar si accedemos a un recurso de red, a un sistema o servidor o documentos. El ataque más típico a la disponibilidad de los sistemas es el de *Denial of Service* (DoS) o ataque de denegación de servicio, que trata de dejar sin servicio a un recurso de una organización. En el capítulo 2 veremos en detalle cuáles son los ataques más comunes que utilizan los tipos malos.

Triángulo de seguridad, funcionalidad y facilidad de uso

Otro concepto formado por tres términos que deberemos recordar es el triángulo de seguridad, funcionalidad y facilidad de uso.



FIGURA 1.15. Triángulo de seguridad, funcionalidad y facilidad de uso.

El triángulo nos muestra la relación entre funcionalidad, seguridad y facilidad de uso. Por ejemplo, si avanzamos hacia la esquina de la seguridad, cuanto más seguro sea algo, más complejo es de usar y menos funcional será (con matices, ya que esto depende del punto de vista, el tipo de negocio o el apetito de riesgo de la compañía). ¿Queremos que un servidor tenga las mejores medidas de protección? No lo conectemos nunca a la red, nunca será atacado, pero entonces perdería toda la funcionalidad para la que un servidor ha sido creado. La idea es encontrar un equilibrio en medio del triángulo, de manera que los tres conceptos se aseguren sin perder ninguno de ellos. Si en el caso de un atacante alguno de estos se ha descuidado, podrá suponer un vector de ataque o una puerta de entrada al sistema.

Enfoque de perímetro de seguridad

La mayoría de los esfuerzos de seguridad se centran en el perímetro de la red en este enfoque. Esto incluye *firewalls*, *proxies*, políticas de contraseñas o cualquier tecnología o procedimiento que haga que los accesos no autorizados a la red sean más complejos. Con este enfoque, el perímetro está totalmente asegurado, pero es posible que los objetos dentro de este sean vulnerables. También tenemos que tener en cuenta la seguridad física en el enfoque de perímetro de seguridad. Esto incluirá vallas, cámaras de seguridad, guardias, cajas fuertes, etc.

Este enfoque solía ser el más común en las organizaciones. Las mismas disponían de su centro de procesos de datos (CPD) con todos sus sistemas conectados bajo el mismo perímetro, tanto servidores como dispositivos de los empleados, y era todo lo que había que proteger. Lo que estaba dentro del perímetro se consideraba seguro *per se* y todo lo que venía de fuera era lo que teníamos que securizar. Durante un tiempo esta estrategia funcionó, como la muralla de un castillo, pero es que nuestro "castillo" ya se ha modernizado y no solo

tenemos nuestros sistemas dentro del mismo, sino que hoy en día pueden estar en cualquier parte del mundo literalmente. Podemos disponer de sistemas *cloud*, que se encuentran en proveedores de *cloud*, de los cuales nos tendremos que ciberpreocupar más o menos en función de la tipología utilizada (SaaS, PaaS o IaaS), como veremos en el capítulo de *cloud*. También existen sistemas de los empleados que trabajan en remoto desde sus casas, no solo PC al uso, sino todo tipo de dispositivos móviles, los cuales también hay que securizar fuera del perímetro. Y, por último, podemos tener proveedores conectados a nuestros sistemas, teniendo que garantizar la seguridad de sus dispositivos y conexiones a las empresas, tanto a nivel tecnológico como a nivel de gobierno y control.

Veremos más adelante, desde la perspectiva del atacante, cómo es posible abordar cada uno de estos flancos. La realidad es que hoy en día están más distribuidos nuestros sistemas y cada vez se hace más difícil proteger los mismos, teniendo que adoptar estrategias como la de Zero Trust Network Access o la emergente SASE.

Zero Trust

Como comentábamos previamente, hemos vivido un cambio de paradigma en los últimos años, donde el *cloud* y el trabajo en remoto han tomado mucho protagonismo. La seguridad perimetral tradicional dependía de *firewalls*, VPN o *gateways* para separar las redes confiables (redes internas) de las que no lo eran (DMZ, Internet o redes de terceros).

La arquitectura de seguridad Zero Trust desconfía de cualquier dispositivo, lugar, persona, etc. Se considera que los dispositivos o las redes siempre pueden estar infectados y se realiza un proceso de verificación siempre de los mismos, así como se mantienen las medidas oportunas como si los mismos estuviesen infectados. Solo se dispone de aplicaciones y datos tomando las siguientes medidas, entre otras:

- A través de autenticación de los usuarios y de todos los dispositivos.
- Se hace monitorización de logs de aplicaciones, sistemas y de tráfico de red de manera proactiva.
- Evitar el *malware* y brechas de seguridad de DNS a través de aplicaciones confiables.
- Controles de acceso dinámicos y contextual a la red, a los sistemas y políticas de mínimo privilegio.

Si unificamos esta estrategia junto con el resto de estrategias de seguridad, los atacantes lo tendrán mucho más complicado, dado que podrían conseguir acceder a una empresa a través de un fallo de seguridad, Zero Day o un descuido, pero, a la hora de hacer movimientos laterales, los diferentes controles ayudarán a que los atacantes se encuentran con más dificultades para perpetrar el ataque.

Defensa en profundidad o enfoque de seguridad por capas

El concepto "defensa en profundidad" se fundamenta en disponer de varias capas de seguridad para el acceso a cualquier recurso de una organización de tal manera que, si saltamos el primer perímetro de seguridad, tengamos que atravesar muchas capas donde nos encontraremos con más controles de seguridad hasta llegar al objetivo final. Por ejemplo, imaginemos que en una organización se restringe el acceso a los datos mediante un control de accesos basado en roles y, para cierta información clasificada como privada o confidencial, se cifran los datos. Si un atacante consigue pasar este primer control de acceso, seguirá sin tener acceso a la información, ya que estará cifrada o no dispondrá del rol adecuado para acceder a esta. Tendremos que disponer tener capas de seguridad tanto en el acceso a los datos, como en los sistemas y en las redes.

Metodologías y estándares en ciberseguridad

Existen diversas metodologías y estándares que intentan normalizar y medir cómo se debería implementar la ciberseguridad en las empresas de cara a **anticiparse, protegerse, detectar, responder y recuperarse** de un ataque o brecha de seguridad. Existen diversos estándares, pero los más conocidos son el estándar ISO/IEC 27001 y el NIST. A efectos formativos, consideramos que el NIST es el más adecuado para nuestros lectores, así que veamos a grandes rasgos qué detalla este marco de controles.

NIST Cybersercurity Framework

El marco de Ciberseguridad NIST proporciona un grupo organizado de políticas para guiar a las organizaciones privadas en cómo se debe organizar la ciberseguridad de las mismas basado en el riesgo. Este marco fue creado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (National Institute of Standards and Technology, NIST) en 2014 y originalmente se creó para la protección de las infraestructuras críticas de EE. UU.

Descripción del marco

El marco trata de reducir el riesgo de las ciberamenazas que pueden comprometer la seguridad de la información de las empresas, estando compuesto por tres partes:

- **Núcleo del marco o *core*:** Se trata de un conjunto de actividades de ciberseguridad, resultados deseados y referencias que son comunes en todos los sectores. Son estándares, directrices y prácticas en la industria de manera que permitan comunicar las actividades y los resultados de ciberseguridad de cualquier organización desde un nivel ejecutivo hasta un nivel de operación. Dispone de 5 funciones: identificar, proteger,

detectar, responder y recuperar. Estas funciones proporcionan una visión estratégica de alto nivel en el ciclo de vida de la gestión de riesgos de una empresa. Estas 5 funciones se dividen en 23 categorías que, a su vez, se subdividen en 108 subcategorías. Cada una de las mismas pretende abordar diferentes dominios de ciberseguridad para tratar de establecer los controles adecuados para la protección de los mismos.

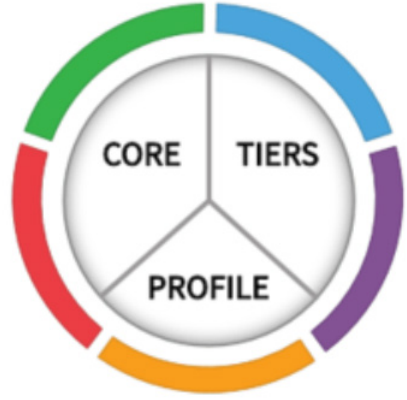


FIGURA 1.16. NIST Cybersecurity Framerwork. Componentes principales.

- **Niveles de implementación del marco, *tiers* o AS-IS:** Dan contexto sobre cómo la empresa considera el riesgo de ciberseguridad y los procesos establecidos para gestionar dichos riesgos, estaríamos hablando del AS-IS, es decir, del estado actual de los controles de ciberseguridad de los que dispone de la compañía en la actualidad. El marco establece 4 niveles de madurez para cada control, desde el más básico (nivel 1) hasta el más maduro (nivel 4). Estos niveles reflejan una progresión desde niveles más básicos disponiendo de controles más manuales hasta niveles más avanzados con controles más maduros y más automatizados.
- **Perfil marco, *profile* o TO-BE:** Se trata de oportunidades para mejorar el escenario de controles o procesos de ciberseguridad, es decir, el estado TO-BE, dónde quiere llegar la empresa a estar para mejorar el estado de su ciberseguridad. El perfil actual o AS-IS se puede utilizar para priorizar y medir el progreso hacia el perfil objetivo o TO-BE.

Núcleo del marco

El *core* o núcleo clasifica las diferentes áreas de la ciberseguridad de las que puede disponer una empresa para poder tomar medidas, establecer controles y ser más resiliente frente ataques. Este consta de funciones, categorías, subcategorías y referencias informativas.

Funciones básicas

El marco se compone de cinco funciones básicas:

- **Identificar o *Identify* (ID):** Comprender el contexto de la organización para evaluar y administrar el riesgo de ciberseguridad de activos, sistemas, personas, datos y capacidades. Para ello es importante conocer la organización, los recursos y funciones críticas para priorizar los esfuerzos en las necesidades y estrategia de riesgos. Un posible ejemplo de herramienta de esta función es el análisis de riesgos, donde se identifican los activos de una entidad, el riesgo asociado a cada uno de ellos, tanto inherente (intrínseco del activo) como residual (riesgo una vez establecidos los controles), y finalmente se establece un plan de acción para eliminar, minimizar o transferir dicho riesgo.
- **Proteger o *Protect* (PR):** Poner en marcha controles de ciberseguridad adecuados, priorizando los servicios críticos de la organización. Esta función está dirigida a evitar un posible ataque, limitando y conteniendo el impacto del mismo lo máximo posible (recordemos que la seguridad 100 % no existe). Herramientas clásicas de esta función son antivirus, *antimalware*, *firewalls*, *gateways*, sistemas anti-DDoS, *Data Loss Prevention* (DLP), etc. En definitiva, cualquier sistema que trate de proteger los activos de los ataques de los tipos malos, ya sean externos o internos (perpetrados por *insiders*).
- **Detectar o *Detect* (DE):** Se trata de desarrollar una estrategia de monitorización de actividades anómalas, preferentemente activa, para poder detectar (lo más en tiempo real posible) un incidente de seguridad. En el caso de haber sufrido un ataque y de que las medidas de protección no hayan sido suficientes, con esta función podemos detectar el ataque en sus inicios pudiendo actuar entonces. Herramientas típicas de este dominio son un *Intrusion Detection System* (IDS), o bien herramientas de detección de amenazas monitorizadas por un SOC (*Security Operations Center*) que detectan anomalías en forma de alertas y evalúan si se trata de un incidente.
- **Responder o *Respond* (RS):** Implementar las actividades adecuadas para tomar las medidas oportunas cuando hemos detectado un incidente de ciberseguridad. Las principales medidas son las de contener el impacto del principal ataque y tratar que el mismo no evolucione. Herramientas relacionadas con esta función pueden ser sistemas *Endpoint Detection and Respond* (EDR), que tratan de actuar en el momento del ataque, o bien cualquier herramienta de análisis forense que trata de desvelar los detalles de lo sucedido.
- **Recuperar o *Recovery* (RC):** Poner en marcha los planes de resiliencia para recuperarnos del ataque y reestablecer las actividades de la compañía que se hayan podido ver comprometidos. Herramientas relacionadas con esta función pueden ir desde los planes de continuidad de negocio (PCN) hasta *backups* de ficheros o de sistemas.



FIGURA 1.17. NIST Cybersecurity Framerwork. Funciones.

Categorías y subcategorías

Como veíamos, las categorías son la subdivisión de una función en grupo vinculadas a las necesidades programáticas y a las actividades particulares. A su vez, estas categorías se dividen en subcategorías, que representan resultados específicos, controles, técnicas o gestión. Algunas de las subcategorías pueden ser "Los sistemas de información externos están catalogados" o "Los datos en reposo están protegidos".

Veamos enumeradas cada una de las categorías del marco.

TABLA 1.1. Categorías del Framework NIST.

FUNCIÓN	CATEGORÍA
Identify (ID)	Asset Management (ID.AM)
Identify (ID)	Business Environment (ID.BE)
Identify (ID)	Governance (ID.GV)
Identify (ID)	Risk Assessment (ID.RA)
Identify (ID)	Risk Management Strategy (ID.RM)
Identify (ID)	Supply Chain Risk Management (ID.SC)
Protect (PR)	Identity Management and Access Control (PR.AC)
Protect (PR)	Awareness and Training (PR.AT)

FUNCIÓN	CATEGORÍA
Protect (PR)	Data Security (PR.DS)
Protect (PR)	Information Protection Processes and Procedures (PR.IP)
Protect (PR)	Maintenance (PR.MA)
Protect (PR)	Protective Technology (PR.PT)
Detect (DE)	Anomalies and Events (DE.AE)
Detect (DE)	Security Continuous Monitoring (DE.CM)
Detect (DE)	Detection Processes (DE.DP)
Respond (RS)	Response Planning (RS.RP)
Respond (RS)	Communications (RS.CO)
Respond (RS)	Analysis (RS.AN)
Respond (RS)	Mitigation (RS.MI)
Respond (RS)	Improvements (RS.IM)
Recover (RC)	Recovery Planning (RC.RP)
Recover (RC)	Improvements (RC.IM)
Recover (RC)	Communications (RC.CO)

Niveles de madurez o TIER

Los niveles de implementación del *framework* NIST (TIER) o niveles de madurez dan contexto sobre cómo la organización considera el riesgo de ciberseguridad y los procesos para gestionar dicho riesgo. Los niveles van desde el nivel más bajo, TIER 1 o parcial, hasta TIER 4 o adaptativo y describen de manera creciente los controles y prácticas de ciberseguridad de cada función y categoría descritos. Estos niveles ayudan a conocer el punto en el que se encuentra una compañía, poder compararse con otras compañías de su mismo sector y establecerse objetivos de mejora para aumentar su nivel de madurez dentro del *framework*.

1. **TIER 1. Parcial:**
   - **Proceso de gestión de riesgos:** Las prácticas de gestión de riesgos no están formalizadas y el riesgo se gestiona *ad hoc*, mayoritariamente, de manera reactiva. La priorización de las actividades de la organización probablemente no esté relacionada con los objetivos de la organización, el entorno y contexto de la misma o los requisitos de negocio.

- **Programa integrado de gestión de riesgos:** Existe una conciencia limitada sobre el riesgo de ciberseguridad en la organización y no se ha establecido un enfoque en la misma de la gestión del riesgo de la ciberseguridad. La organización implementa la gestión del riesgo de manera errática, caso por caso, debido a la experiencia o información de fuentes externas. La organización no tiene procesos que permitan compartir información de ciberseguridad en la organización.
- **Participación externa:** La organización no tiene procesos establecidos para participar en la coordinación o colaboración con otras entidades en materia de ciberseguridad.

2. **TIER 2. Riesgos de información:**
   - **Proceso de gestión de riesgos:** Las prácticas de gestión de riesgos son aprobadas por la administración, pero no pueden establecerse como políticas de toda la organización. Las actividades se priorizan con los objetivos de la organización, el entorno y contexto de la misma o los requisitos de negocio.
   - **Programa integrado de gestión de riesgos:** Existe una conciencia del riesgo de ciberseguridad en la organización, pero no se ha puesto en marcha un enfoque en toda la organización para gestionar el riesgo de ciberseguridad. Los procesos y procedimientos informados por el riesgo se aprueban por la gerencia, se implementan y los empleados cuentan con los recursos adecuados para realizar las tareas de ciberseguridad. La información de ciberseguridad se comparte en la organización de manera formal.
   - **Participación externa:** La organización conoce su rol en el ecosistema mayor, pero no ha formalizado sus capacidades para interactuar y compartir información con otras organizaciones o instituciones.
3. **TIER 3. Repetible:**
   - **Proceso de gestión de riesgos:** Las prácticas de gestión de riesgos se aprueban formalmente y se traspasan a políticas. Las prácticas de ciberseguridad se actualizan periódicamente en función de la aplicación de los procesos de gestión de riesgos a los cambios en la estrategia de la organización, la misión y un entorno y contexto cambiantes, tanto tecnológicos como de amenazas.
   - **Programa integrado de gestión de riesgos:** En toda la organización existe un enfoque de gestión de riesgo de ciberseguridad. Existen políticas, procesos y procedimientos informados sobre riesgos. Los empleados poseen el conocimiento y las habilidades para conocer sus roles y responsabilidades asignadas.
   - **Participación externa:** La organización entiende sus dependencias con otras organizaciones, da y recibe información de los mismos, colabora y toma decisiones de gestión de riesgo basadas en dicho intercambio de información.

4. **TIER 4. Adaptable:**
    - **Proceso de gestión de riesgos:** La organización adapta sus prácticas de ciberseguridad en base a lecciones aprendidas y a indicadores predictivos. A través de un proceso de mejora continua, que pone en marcha prácticas y tecnologías avanzadas, la organización se adapta proactivamente a un entorno cambiante, respondiente a las amenazas cambiantes y sofisticadas.
    - **Programa integrado de gestión de riesgos:** En toda la organización se gestiona el riesgo de ciberseguridad, usando políticas, procesos y procedimientos informados. La gestión del riesgo de ciberseguridad forma parte de la cultura de la organización y evoluciona a partir de la conciencia de las actividades previas, la información compartida por otras fuentes y el conocimiento continuo de las actividades de sus sistemas y redes.
    - **Participación externa:** La organización gestiona los riesgos y comparte activamente información con otras organizaciones para garantizar que la información esté actualizada, se distribuya y se consuma para mejorar la ciberseguridad en el sector.

Establecer un plan de acción o programa de ciberseguridad

¿Cómo puede una organización utilizar el *framework* del NIST para crear un programa de ciberseguridad o mejorar el ya existente? Veamos los siguientes pasos que podrían orientar a ello.

1. **Definir el alcance:** Identificar cuál es la misión de la organización, cuáles son sus prioridades y cuáles son los activos y procesos más importantes a alto nivel. Con esta información, se toman decisiones estratégicas respecto a la implementación de ciberseguridad y se determina el alcance de los sistemas, activos y personas a evaluar.
2. **AS-IS:** Previo a hacer la evaluación se crea un perfil de cómo está la organización en materia de ciberseguridad en cada una de las funciones, categorías y subcategorías del NIST. A estas se les pone una puntuación o nivel de madurez.
3. **Evaluación de riesgos:** Siguiendo el proceso de gestión de riesgos de la organización y el *framework* del NIST, se analiza el entorno para anticipar un posible evento de ciberseguridad y su impacto. Se incorporan al análisis los riesgos emergentes, datos de amenazas y vulnerabilidades actuales, para facilitar el análisis de probabilidad e impacto de los eventos de ciberseguridad.
4. **TO-BE:** Una vez evaluado el escenario actual y conocidas las prioridades de la organización, se crea un perfil de dónde la organización quiere estar en un futuro en cada una de las funciones, categorías y subcategorías del NIST.

5. **Analizar y priorizar actividades:** Se analiza la diferencia entre el AS-IS y el TO-BE, las actividades, tareas y controles que son necesarias y se priorizan las mismas en un plan de acción, teniendo en cuenta un análisis de costes y beneficios de la misma en base al riesgo y los resultados que se quieren obtener.
6. **Poner en marcha el plan de acción:** Una vez determinadas las acciones que hay que realizar y priorizadas, se ejecuta el plan de acción y se evalúa de manera periódica para realizar seguimiento del mismo o bien adaptarlo.

Recursos de seguridad *online*

Qué mejor manera de estar actualizados con las últimas novedades en seguridad que mediante los recursos que podemos encontrar en Internet, los cuales nos ayudarán a conocer mejor el entorno. Algunos de estos se tratan de organizaciones gubernamentales, creadas para velar por la seguridad de los ciudadanos; otros son empresas que ponen a nuestra disposición gran cantidad de información acerca de la seguridad de la información, y otros muchos son blogs de personas implicadas en el mundo de la seguridad, que aportan información muy útil basada en su experiencia y conocimiento.

Veamos algunos de estos recursos que tenemos en la red:

- **CERT, Computer Emergency Response Team:** Fue el primer equipo de respuesta a incidentes de seguridad y sigue siendo uno de los más respetados en la industria. Fue creado por la Universidad Carnegie-Mellon en la ciudad de Pittsburgh en Pensilvania, Estados Unidos. En su página web, `http://www.cert.org`, se puede encontrar multitud de documentación, así como *guidelines* de políticas de seguridad, investigaciones de seguridad y otros. Este equipo de trabajo ha desarrollado un modelo de CERT que es replicado en multitud de organizaciones a nivel mundial (tanto públicas como privadas) y que consigue el sello oficial a través de un proceso de certificación evaluado por ellos.
- **CCN-CERT, CERT Gubernamental Español:** Es equiparable al US-CERT estadounidense. Según indican en su página web, `https://www.ccn-cert.cni.es/`, "es la capacidad de respuesta a incidentes de seguridad de la información del **Centro Criptológico Nacional**. Este servicio se creó a finales del año 2006 como CERT gubernamental español, y sus funciones quedan recogidas en el capítulo VII del RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. Este texto legal, en su artículo 37, señala los servicios que el CCN-CERT ya prestaba desde su constitución (en parte recogidos en el RD 421/2004 de regulación del CCN)". El Centro Criptológico Nacional vela por que las instituciones públicas cumplan unos niveles mínimos de seguridad. La idea es que sirva de centro de alerta nacional que