CIBERSEGURIDAD

MANUAL PRÁCTICO



ECOE EDICIONES

Paraninfo

José Manuel Ortega Candel

Ciberseguridad

Manual práctico

José Manuel Ortega Candel

Catalogación en la publicación - Biblioteca Nacional de Colombia

Ortega Candel, José Manuel, autor
Ciberseguridad : manual práctico / José Manuel Ortega Candel. -- Primera edición. -- Bogotá : Ecoe Ediciones ; Madrid : Ediciones Paraninfo, 2024.
335 páginas. -- (Computación y tecnología de la información. Seguridad informática)

Incluye datos curriculares del autor.

ISBN 978-958-503-839-4 -- 978-958-503-840-0 (e-book)

1. Seguridad informática - Manuales 2. Internet - Medidas de seguridad - Manuales 3. Protección de datos - Manuales

CDD: 005.8 ed. 23 CO-BoBN– a1133895

Área: *Computación y tecnología de la información*
Subárea: *Seguridad informática*

ECOE EDICIONES

Paraninfo

© José Manuel Ortega Candel

© Ediciones Paraninfo, SA
info@paraninfo.es
www.paraninfo.es
Teléfono: (+34) 914 463 350
Calle José Abascal 41,
Oficina 701. 28003
Madrid, España

© Ecoe Ediciones S.A.S.
info@ecoeediciones.com
www.ecoeediciones.com
Carrera 19 # 63 C 32
Teléfono: (+57) 321 226 46 09
Bogotá, Colombia

Primera edición: Bogotá, enero del 2024

ISBN: 978-958-503-839-4
e-ISBN: 978-958-503-840-0

Directora editorial: Ana María Rueda G.
Coordinadora editorial: Paula Bermúdez B.
Editora de adquisiciones: Alejandra Cely R.
Carátula: Wilson Marulanda Muñoz
Impresión: Xpress Estudio Gráfico y Digital
Carrera 69 H # 77 - 40

Prohibida la reproducción total o parcial por cualquier medio sin la autorización escrita del titular de los derechos patrimoniales.

Impreso y hecho en Colombia - Todos los derechos reservados

Contenido

1. INTRODUCCIÓN A LA CIBERSEGURIDAD 1

1.1. Diferencia entre seguridad de la información y ciberseguridad 2
1.2. Objetivos de la ciberseguridad 3
1.2.1. Confidencialidad. 4
1.2.2. Integridad 5
1.2.3. Disponibilidad 7
1.2.4. Resumen. 8
1.3. Personas y roles en ciberseguridad 8
1.3.1. Profesionales de la ciberseguridad 9
1.3.2. Gerente de seguridad de la información 11
1.3.3. Gobierno de la ciberseguridad 12
1.4. Dominios de la ciberseguridad 13
1.4.1. Conceptos de ciberseguridad 14
1.4.2. Principios de arquitectura de ciberseguridad. 14
1.4.3. Seguridad de redes, sistemas, aplicaciones y datos 15
1.4.4. Respuesta a incidentes 15
1.4.5. Dominios de seguridad según el estándar ISO 27000 15
1.5. Gestión de riesgos y controles de ciberseguridad. 16
1.5.1. Gestión de riesgos. 17
1.5.2. Controles de ciberseguridad 18
1.6. *Frameworks* de ciberseguridad 21
1.6.1. *Framework* de ciberseguridad NIST. 21
1.6.2. Controles de ciberseguridad NIST 24
1.6.3. Controles de ciberseguridad CIS 26
Enlaces web de interés 27
Actividades finales. 28

2. SEGURIDAD EN LA NUBE 31

2.1. Introducción a la computación en la nube (*cloud computing*) 32
2.2. Modelos de servicios en la nube (IaaS, PaaS, SaaS) 34
2.2.1. *Software as a service* (SAAS) 35
2.2.2. *Platform as a service* (PAAS) 36
2.2.3. *Infrastructure as a service* (IAAS) 37
2.3. Seguridad en la nube. 38
2.3.1. Riesgos de computación y aplicaciones en la nube. 42

2.4. Cifrado de la información en la nube 43
2.4.1. Tipos de cifrado 44
2.4.2. El cifrado en la nube: proveedor y cliente 45
2.5. Herramientas de cifrado de archivos 46
2.5.1. Boxcryptor 47
2.5.2. Cryptomator 47
2.5.3. Spideroak 48
2.5.4. Tresorit 48
2.5.5. Nextcloud 49
2.5.6. Owncloud 51
2.5.7. Otras soluciones 52
2.5.8. Conclusiones sobre la nube privada 53
2.6. Uso de certificados de forma segura 53
2.6.1. El protocolo SSL 54
2.6.2. Ejemplo de certificado seguro 55
2.6.3. Let's Encrypt 56
Enlaces web de interés 57
Actividades finales 58

3. SEGURIDAD EN INTERNET 61

3.1. Tipos de amenazas y ataques en internet 62
3.1.1. Ciberamenazas 63
3.1.2. Principales amenazas de ciberseguridad 64
3.2. Introducción al *malware* y tipos 66
3.2.1. Troyanos 68
3.2.2. Clasificación de los *rootkits* 69
3.2.3. *Keyloggers* y *screen scrapers* 70
3.2.4. *Botnets* 70
3.2.5. Identificación de *malware* 72
3.3. Amenazas persistentes avanzadas (APT) y ataques dirigidos 74
3.3.1. Métodos de infección 75
3.3.2. Ataques de denegación de servicio 78
3.3.3. Ataques de correo electrónico y *cookies* 80
3.3.4. Ataques de DNS (sistema de nombres de dominio) 81
3.3.5. *Ransomware* 83
3.4. Protección de los sistemas frente a las amenazas 85
3.4.1. Protección de las infraestructuras críticas 87
3.4.2. Protección frente a ataques DDoS 88
3.4.3. Protección frente a ataques DNS 89
3.5. Protección frente a amenazas persistentes avanzadas 91
3.6. Protección frente a *malware* (virus, troyanos, *spyware, rootkits*) 93
3.6.1. Uso de un antivirus 95
3.6.2. Protección *antibotnet* 95
3.6.3. Detección de *malware* en Linux con LMD (Linux Malware Detect) 96
Enlaces web de interés 98
Actividades finales 99

4. PRIVACIDAD EN INTERNET 101

4.1. Introducción a la privacidad 102
4.2. Privacidad de información en la nube 104
4.2.1. VPN (red privada virtual) 104
4.2.2. Proveedores VPN 106
4.2.3. OpenVPN 107

4.3. Privacidad en dispositivos IoT (*Internet of Things*) 108
4.3.1. Tendencias de privacidad en IoT en las organizaciones. 110
4.4. Privacidad en los navegadores. 111
4.4.1. Herramientas para el control de las *cookies* 112
4.5. Conexión con la red Tor 115
4.5.1. Navegador Tor Browser 116
4.5.2. Navegación anónima en la red Tor 119
4.6. Navegadores y buscadores alternativos 120
4.6.1. Brave. 121
4.6.2. DuckDuckGo 122
4.6.3. Buscadores alternativos. 124
Enlaces web de interés 127
Actividades finales. 128

5. SEGURIDAD EN APLICACIONES WEB 131

5.1. Metodología OWASP 132
5.2. Ataques en aplicaciones web 133
5.2.1. Vectores de ataque 136
5.2.2. XSS (*Cross-Site Scripting*) 137
5.2.3. CSRF (*Cross-Site Request Forgery*) 142
5.2.4. Seguridad en las redirecciones 143
5.2.5. Autenticación y manejo de sesiones 144
5.3. SQL Injection: parametrización de las consultas en bases de datos 147
5.3.1. Introducción a SQL injection 147
5.3.2. Problemas que pueden causar este tipo de ataques. 147
5.3.3. Ejemplo de SQL injection 148
5.3.4. Escapar los caracteres especiales utilizados en las consultas SQL 150
5.3.5. Uso de sentencias preparadas parametrizadas. 151
5.4. Herramientas para capturar las peticiones en aplicaciones web 152
5.4.1. OWASP ZAP. 152
5.4.2. BurpSuite 160
5.4.3. Fiddler 162
5.5. sqlmap 163
Enlaces web de interés 168
Actividades finales. 169

6. DESARROLLO SEGURO DE APLICACIONES 173

6.1. Introducción al desarrollo seguro 174
6.2. Ciclo de vida de desarrollo de *software* (SDLC) 175
6.3. Desarrollo y operaciones TI (DevOps) 176
6.3.1. DevSecOps. 178
6.3.2. Seguridad por diseño 181
6.4. Requisitos de seguridad en las aplicaciones. 181
6.5. Arquitectura segura en las aplicaciones. 183
6.5.1. Autenticación 183
6.5.2. Gestión de sesiones. 184
6.5.3. Control de acceso 184
6.5.4. Validación de entradas 185
6.5.5. Codificación de salida y rutinas de escape 185
6.5.6. Criptografía. 185
6.5.7. Gestión de errores y *logging* 186
6.5.8. Protección de datos. 186
6.5.9. Seguridad en las comunicaciones 187

6.5.10. Seguridad en el protocolo HTTPS . . . 187
6.5.11. Codificación segura en las aplicaciones . . . 188
6.6. Herramientas de pruebas de seguridad . . . 188
6.6.1. OSSTMM (*Open Source Security Testing Methodology Manual*) . . . 189
6.6.2. Auditorías de seguridad del código . . . 189
6.6.3. Revisión de código automatizada . . . 190
6.6.4. Análisis estático seguro de código (SAST) . . . 191
6.6.5. Análisis de dependencias . . . 193
6.6.6. Pruebas dinámicas de seguridad (DAST) . . . 194
6.7. Principales vulnerabilidades del *software* . . . 195
6.7.1. Desbordamiento de memoria en C/C++ (desbordamiento de búfer) . . . 197
6.7.2. Análisis de funciones vulnerables . . . 202
6.7.3. Vulnerabilidad de validación de entrada . . . 204
Enlaces web de interés . . . 206
Actividades finales . . . 207

7. *HACKING* ÉTICO Y HERRAMIENTAS DE ANÁLISIS DE RED 211

7.1. Introducción al *hacking* ético . . . 212
7.1.1. Tipos de *hacking* ético . . . 213
7.1.2. Fases de un *hacking* ético . . . 214
7.2. Introducción a las auditorías . . . 215
7.2.1. Estándares de auditoría informática . . . 215
7.2.2. Tipos de auditorías . . . 216
7.3. Auditoría de sistemas y redes . . . 217
7.3.1. Comprobar la seguridad de un servidor SSH . . . 217
7.3.2. Rebex SSH Check . . . 218
7.3.3. ssh-audit . . . 219
7.3.4. Auditoría de redes . . . 221
7.3.5. Ataques de hombre en el medio (MITM) . . . 222
7.3.6. Ataques de denegación de servicio (DOS) . . . 224
7.3.7. Ataque DNS *spoofing* . . . 225
7.4. Nmap como escáner de puertos . . . 226
7.4.1. Técnicas de escaneo de puertos . . . 228
7.4.2. Detección del sistema operativo y aplicaciones . . . 231
7.4.3. Optimizar el escaneo de puertos . . . 233
7.4.4. Análisis de vulnerabilidades con nmap . . . 233
7.5. Escáneres de seguridad *open source* . . . 234
7.5.1. Arachni . . . 235
7.6. Escáneres de red . . . 239
7.6.1. Zenmap . . . 239
7.7. Herramientas de análisis de tráfico de red . . . 242
7.7.1. Wireshark . . . 243
7.7.2. NetworkMiner . . . 245
Enlaces web de interés . . . 248
Actividades finales . . . 249

8. INTRODUCCIÓN A LA INTELIGENCIA DE FUENTES ABIERTAS (OSINT) 251

8.1. Introducción a OSINT . . . 252
8.1.1. Ciclo de vida de OSINT . . . 252
8.1.2. OSINT frente a investigación . . . 253
8.1.3. Fuentes públicas OSINT . . . 253
8.2. OSINT como disciplina de inteligencia . . . 255
8.2.1. El proceso de inteligencia . . . 256

8.2.2. Disciplinas de inteligencia . . . 256
8.2.3. Incidentes e investigaciones . . . 258
8.2.4. Métodos de recolección de información . . . 258
8.3. *Hacking* con buscadores . . . 260
8.3.1. Google CSE (*Custom Search Engine*) . . . 260
8.3.2. Google Hacking Database . . . 261
8.3.3. Google Dorks . . . 262
8.3.4. Búsqueda avanzada en Google y Bing con Advangle . . . 264
8.4. Motores de búsqueda alternativos . . . 265
8.4.1. Shodan . . . 266
8.4.2. Censys y ZMap . . . 268
8.4.3. Binaryedge . . . 270
8.4.4. Otros motores de búsqueda . . . 270
8.5. Herramientas OSINT . . . 272
8.5.1. Recopilación de información o *footprinting* . . . 274
8.5.2. theHarvester . . . 276
8.5.3. Escáner de puertos . . . 277
8.5.4. Identificación de la infraestructura y de los rangos de red . . . 278
8.6. Herramientas para obtener información sobre un dominio . . . 280
8.6.1. Enumeración de subdominios . . . 282
8.6.2. Obtener subdominios con Nmap . . . 284
8.6.3. Extracción de subdominios con Sublist3r . . . 285
8.7. Extracción de metadatos de documentos con ExifTool . . . 286
Enlaces web de interés . . . 288
Actividades finales . . . 290

9. CENTRO DE OPERACIONES DE SEGURIDAD (SOC) 293

9.1. Introducción al centro de operaciones de seguridad (SOC) . . . 294
9.1.1. Vectores para construir un SOC . . . 294
9.1.2. Características y construcción de un SOC . . . 295
9.2. Respuesta a incidentes de ciberseguridad . . . 296
9.2.1. Preparación . . . 297
9.2.2. Detección y análisis . . . 297
9.2.3. Contención y recuperación . . . 298
9.2.4. Actividades posincidente . . . 299
9.3. Gestión de vulnerabilidades . . . 300
9.3.1. Análisis de vulnerabilidades . . . 300
9.3.2. Repositorios de vulnerabilidades . . . 304
9.3.3. Explotación de vulnerabilidades . . . 308
9.4. Herramientas SIEM de monitorización de *logs* . . . 309
9.4.1. Introducción a los SIEM . . . 309
9.4.2. Gestión de eventos en los SIEM . . . 310
9.4.3. Ventajas de los SIEM . . . 311
9.4.4. Introducción al ELK Stack . . . 313
9.4.5. Otro *software* SIEM . . . 319
9.5. Sistemas de detección de intrusos (IDS) . . . 319
9.5.1. Limitaciones de los IDS . . . 320
9.5.2. Tipos de sistemas de detección de intrusos . . . 321
9.5.3. Snort como sistema de detección de intrusos . . . 324
9.6. Otras herramientas que actúan como IDS . . . 331
Enlaces web de interés . . . 333
Actividades finales . . . 334



Introducción a la ciberseguridad

La protección de la información es una función crítica para todas las empresas, industrias y sociedades modernas. Salvaguardar la información ha sido una prioridad desde que las personas han necesitado mantener la información de una forma segura y privada. La ciberseguridad es un campo cada vez más amplio y cambiante, y es crucial que los conceptos centrales que enmarcan y definen este campo sean entendidos por los profesionales que estén interesados e involucrados en las implicaciones de seguridad de las tecnologías de la información (TI).

Mientras que el panorama de la ciberseguridad ha evolucionado, el conjunto de habilidades entre los profesionales de la ciberseguridad, existentes o potenciales, no lo ha hecho al mismo ritmo. Asimismo, algunos estudios creen que el creciente déficit de capacidades en ciberseguridad está amenazando la competitividad de la Unión Europea y las brechas de habilidades se observan tanto en aspectos técnicos como en aspectos de negocio de la seguridad.

Contenidos

1.1. Diferencia entre seguridad de la información y ciberseguridad
1.2. Objetivos de la ciberseguridad
1.3. Personas y roles en ciberseguridad
1.4. Dominios de la ciberseguridad
1.5. Gestión de riesgos y controles de ciberseguridad
1.6. *Frameworks* de ciberseguridad

1.1. DIFERENCIA ENTRE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Desde hace poco más de 50 años asistimos a una revolución que nos ha introducido en la era de la información y del conocimiento, y que está propiciada por el uso masivo de sistemas de información y redes de ordenadores. Sus rasgos distintivos son la rapidez con la que se ha extendido y la profundidad de los cambios que está provocando en la sociedad e incluso en la vida de las personas.

Por eso, dependemos críticamente de estos sistemas, de modo que su inoperatividad o mal funcionamiento, accidental o deliberado, comporta graves consecuencias, incluso para la sociedad en general junto con los servicios esenciales imprescindibles para el funcionamiento de la misma. Por ejemplo, un informe del estado de ciberseguridad en la Unión Europea en 2020 indica que en algunos países los incidentes de seguridad superan el 50 % del total y el 80 % de las empresas habían sufrido al menos un incidente de este tipo.

La **ciberseguridad** se ocupa de la protección de los activos digitales, incluyendo redes, *hardware* y *software*, así como la información que es procesada, almacenada en sistemas o transportada a través de entornos de información interconectados, y nos referimos al conjunto de técnicas, sistemas de gestión y otras medidas que pretenden proteger la información digital y los medios que la tratan de incidentes deliberados o accidentales.

En cambio, la **seguridad de la información** trata con la información, independientemente del formato en que la estemos manejando, incluyendo documentos en papel, propiedad digital e intelectual, así como las comunicaciones verbales o visuales.

Podríamos pensar en la ciberseguridad como un componente de la seguridad de la información. De esta forma podríamos definir el término ciberseguridad como la **protección de activos de información que aborda las amenazas a la información procesada, almacenada y transportada a través de los sistemas de información interconectados.**

En resumen, la principal diferencia con respecto a la seguridad de la información es que esta trata de proteger esa información independientemente de cuál sea su soporte (papel, digital) o forma de tratamiento (manual o automatizada).

En el núcleo del marco de ciberseguridad podemos identificar **cinco funciones clave** necesarias para la protección de los activos digitales en las organizaciones. Estas funciones coinciden con metodologías de gestión de incidentes e incluyen las siguientes actividades:

- **Identificar:** usar el entendimiento de la organización para minimizar el riesgo de los sistemas, activos, datos y capacidades.
- **Proteger:** diseñar salvaguardas para limitar el impacto de los eventos potenciales en servicios e infraestructuras críticos.
- **Detectar:** implementar actividades para identificar la presencia de eventos de ciberseguridad.

- **Responder:** tomar las medidas adecuadas tras conocerse un evento de seguridad.
- **Recuperar:** planificar para tener resiliencia y recuperar de forma oportuna los servicios y capacidades que pudieran haber sido comprometidos.

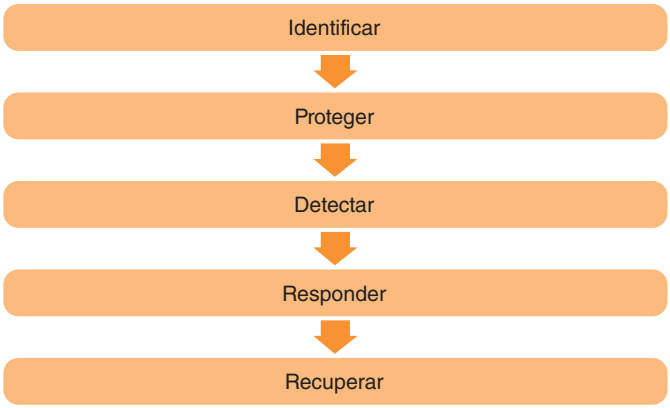


Figura 1.1. Principales actividades de ciberseguridad.

RECUERDA

La definición de ciberseguridad según ISACA (https://www.isaca.org) es la «protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados».

La ciberseguridad se encarga tanto de las amenazas internas como de las externas a los activos de información digital de una organización, centrándose en los procesos críticos de datos electrónicos, el procesamiento de transacciones, el análisis de riesgo y la ingeniería de seguridad de los sistemas de información.

Hoy en día se estima que hay entre 500 000 y 600 000 profesionales de seguridad de la información en todo el mundo, y se espera que la demanda pueda aumentar un 70 % en los próximos años con más de 5 millones de puestos de trabajo disponibles.

1.2. OBJETIVOS DE LA CIBERSEGURIDAD

La ciberseguridad tiene como propósito cumplir ciertos objetivos en la protección de los activos digitales. Para entender mejor la ciberseguridad y la protección de activos digitales, es útil tener en cuenta **tres conceptos clave** que se utilizan para guiar las políticas de seguridad de la información. Mantener un sistema seguro consiste en garantizar los **principios** de confidencialidad, integridad y disponibilidad de los activos, entre otros aspectos.

- **Confidencialidad:** principio que indica que solo pueden acceder a los recursos de un sistema los usuarios autorizados.
- **Integridad:** es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales. Indica que los recursos del sistema solo pueden ser modificados por los usuarios autorizados.
- **Disponibilidad:** se trata de la capacidad de un servicio, un sistema o una información a ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran. Los recursos del sistema tienen que estar a disposición de los usuarios autorizados.

Para determinar si un usuario está o no autorizado para llevar a cabo determinadas tareas dentro del sistema se necesitan, además, otros servicios de ciberseguridad entre los que podemos destacar:

- **Autenticidad:** consiste en poder confirmar la identidad de un usuario. El ejemplo más habitual es la introducción de usuario y contraseña para comenzar a utilizar un sistema o un servicio web.
- **Control de acceso:** especifica qué acciones pueden llevar a cabo los usuarios del sistema.
- **No repudio/autenticidad:** el no repudio en el envío de información a través de las redes es la capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.
- **Trazabilidad:** se trata del conjunto de procesos, técnicas y herramientas que permiten conocer el histórico, la ubicación y la trayectoria de un dato, conjunto de información o transacción a lo largo de la cadena de suministros en un momento dado. Es decir, saber dónde ha estado, quién ha accedido y/o modificado el dato, etcétera.

A continuación pasamos a detallar los principios comentados anteriormente.

1.2.1. CONFIDENCIALIDAD

La confidencialidad está enfocada en restringir el acceso a personas no autorizadas y se refiere a la protección de la información con el objetivo de prevenir el acceso no autorizado o la divulgación de la misma.

Para comenzar, la información más sensible necesita estar protegida por sistemas de seguridad vigentes que empleen las mejores medidas de seguridad del mercado. Entre las distintas herramientas de protección de datos que aseguran que los usuarios no obtendrán la información de manera ilícita se encuentran: uso de contraseñas, segundo factor de autenticación, cifrado y clasificación de datos, uso de sistemas biométricos y *tokens* de seguridad. De esta forma, la confidencialidad puede ser preservada utilizando los siguientes métodos:

- **Controles y registros de acceso.**
- **Permisos sobre los archivos.**
- **Cifrado en ficheros y sistema de archivos.**

1.2.2. INTEGRIDAD

La integridad se refiere a cómo los datos se mantienen intactos, libres de modificaciones o alteraciones por terceros; y en el mundo digital también es aplicable a correos electrónicos, archivos, *software* y configuraciones en las aplicaciones.

Por este motivo se debe proteger la información para que solo sea modificada por aquellos usuarios que tengan los permisos adecuados, evitando así que se pierda la integridad. Una manera de proteger los datos es cifrando la información mediante un método de autenticidad, como una contraseña o mediante huella digital utilizando alguno de los siguientes métodos:

- **Controles y registros de acceso.**
- **Permisos sobre los archivos.**
- **Cifrado en ficheros y sistema de archivos.**
- **Realización de copias de seguridad.**
- **Uso de firmas digitales.**
- **Uso de resúmenes criptográficos utilizando funciones *hash*.**

Entre las distintas maneras de asegurar la integridad de la información se encuentra la práctica de realizar copias de seguridad, ya sea en los propios servidores de la empresa o en la nube. Para la verificación del estado de la información se suelen utilizar herramientas que permiten obtener el ***hash*** para detectar cualquier cambio realizado en los archivos.

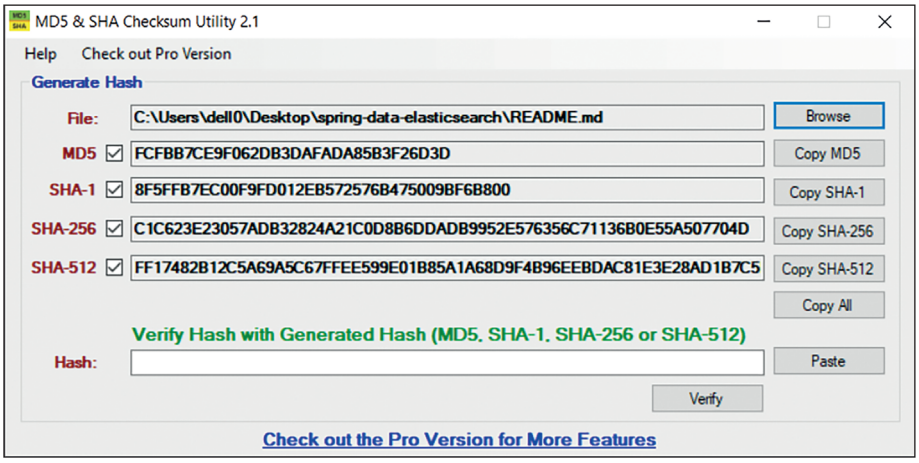


Figura 1.2. Utilidad que permite obtener el *hash* de un fichero con diferentes algoritmos.

NOTA TÉCNICA

El *hash* de un fichero se refiere a la suma de comprobación de este y permite determinar si el archivo se ha visto modificado. Se trata de un método que usa unos algoritmos específicos para comprobar la integridad del archivo y tener la certeza de que no ha sido manipulado y es totalmente confiable. Entre los principales algoritmos que se usan para calcular este valor podemos destacar:

- **MD5 (*Message-Digest Algorithm 5*, algoritmo de resumen del mensaje 5):** es un algoritmo criptográfico de 128 bits y uno de los más usados actualmente.
- **SHA-1 (*Secure Hash Algorithm*, algoritmo de *hash* seguro):** es un conjunto de funciones *hash* muy usado en aplicaciones de firma electrónica ya que genera códigos *hash* de entre 160 y 254 bits.
- **SHA-256:** es uno de los algoritmos más usados en diversos protocolos por su alcance a nivel de seguridad, tales como TLS, SSL, PGP y SSH, entre otros.

Entre las principales herramientas de que disponemos para obtenerlos podemos destacar:

- **MD5 & SHA Checksum Utility:**
  https://raylin.wordpress.com/downloads/md5-sha-1-checksum-utility
- **HashTab:**
  http://implbits.com/products/hashtab/

La obtención de la firma de un fichero es un aliado a nivel de seguridad y protección de nuestros equipos ya que nos permite detectar si ha habido una manipulación de los archivos descargados.

La integridad de la información permite garantizar que esta no ha sido modificada en cualquiera de sus tres estados (en almacenamiento, en proceso o en tránsito) y analizarlo desde perspectivas distintas con el objetivo de:

- Prevenir que alguien con permisos de modificación pueda hacerlo de forma errónea.
- Prevenir que alguien sin permisos de modificación realice algún cambio.
- Prevenir que alguna aplicación que interactúa directamente con la información realice algún cambio sobre esta última.

Como vemos, hay puntos en común con respecto a los de confidencialidad, añadiendo además la realización de copias de seguridad, el uso de firmas digitales y la obtención de resúmenes criptográficos utilizando funciones *hash*.

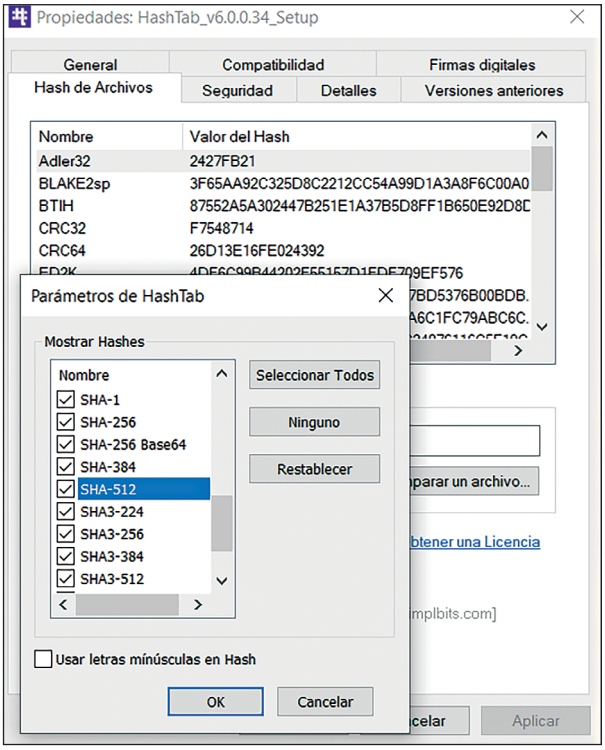


Figura 1.3. En el caso de la utilidad HashTab podemos obtener el *hash* usando diferentes algoritmos de comprobación.

1.2.3. DISPONIBILIDAD

La disponibilidad garantiza el acceso oportuno y confiable al uso de la información y los sistemas. Esto incluye la realización de copias de seguridad para asegurar que los datos no se eliminan de forma accidental o malintencionada. Esto es particularmente importante en sistemas críticos, ya que cualquier interrupción en su disponibilidad puede resultar en una pérdida del servicio que se está proporcionando.

Este concepto no solo habla del sistema operativo y de los *softwares* necesarios, sino también del mantenimiento del *hardware*, las redes, los dispositivos y la protección en general de los equipos físicos utilizados para llevar a cabo los procesos de almacenamiento de la información.

Del mismo modo, la pérdida de datos puede afectar a la capacidad de las organizaciones para tomar decisiones y respuestas efectivas. La disponibilidad puede ser preservada utilizando los siguientes métodos:

- **Redundancia en redes y sistemas.**
- **Replicación de datos.**

- **Realización de copias de seguridad.**
- **Controles de acceso.**
- **Definición de un plan de recuperación de desastres o plan de continuidad del negocio.**

1.2.4. RESUMEN

En resumen, la **confidencialidad** implica protección contra el acceso no autorizado, la **integridad** implica protección contra modificaciones no autorizadas, y la **disponibilidad** implica protección frente a las interrupciones en el acceso a la información. No obstante, otras fuentes añaden otras como la **autenticidad** (que la información provenga de una fuente), el **no repudio** (que el autor no pueda rechazar su autoría) y la **trazabilidad** (que pueda rastrearse su ciclo de vida).

Las primeras tres propiedades de seguridad de la información dependen una de otra de la siguiente forma:

- Si no se tiene confidencialidad, la probabilidad de que se viole la integridad de la información aumenta potencialmente, dando pie a que un usuario no autorizado pueda modificar la información.
- Si se modifica la integridad de los datos, entonces la información o aplicaciones clave del negocio se verán afectadas y no podrán dar el servicio esperado, lo que llevaría a un impacto en la disponibilidad.

Realizar una correcta gestión de la seguridad de la información establece como principio básico que sin los tres elementos mencionados no existe nada seguro y con que solo falle uno de los componentes nos encontramos ante un peligro para nuestra seguridad de la información.

A continuación, vamos a detallar los principales roles y cargos que describen algunas de las funciones específicas en ciberseguridad que podemos encontrar en la mayoría de las organizaciones.

1.3. PERSONAS Y ROLES EN CIBERSEGURIDAD

La ciberseguridad es un campo que demanda profesionales cualificados que posean los conocimientos básicos y el liderazgo necesario para hacer frente a las dificultades que acompañan el cambio tecnológico constante y dinámico. Los vectores de amenazas avanzados y las tecnologías emergentes requieren de profesionales de la ciberseguridad expertos en tecnología, así como en negocios y en comunicación.

Debido a que la ciberseguridad es parte de la seguridad de la información, en algunas ocasiones hay una superposición entre los términos y la forma en que son aplicados a las estructuras de gestión y los diferentes roles. Para los propósitos de esta unidad asumimos

que el término seguridad de la información abarca los roles y las funciones de la ciberseguridad.

1.3.1. PROFESIONALES DE LA CIBERSEGURIDAD

En la mayoría de las organizaciones la ciberseguridad es gestionada por un equipo de expertos en la materia y por profesionales en ciberseguridad, incluyendo arquitectos de seguridad, administradores, forenses digitales, administradores de incidentes, investigadores de vulnerabilidades y especialistas en seguridad de las redes.

A continuación, vamos a analizar una lista que incluye los perfiles más característicos del sector de la seguridad informática y que comparten la esencia, pero luego cada perfil se especializa en distintos ámbitos. También es importante destacar que lo interesante de esta industria es que la mayoría de los perfiles se encuentran interconectados en algún nivel. Entre los principales roles de ciberseguridad podemos destacar estos:

- ***Chief Security Officer* (CSO).** Se trata del perfil de mayor responsabilidad a nivel ejecutivo en seguridad digital de una empresa y normalmente cuenta con amplios conocimientos legales y técnicos, además de empresariales, que le permiten desenvolverse tanto en la prevención de riesgos como en los propios ataques. Se ocupa de establecer los planes de continuidad de negocio y recuperación de desastres, comprender las necesidades normativas y asegurarse de que todas las actividades son planificadas y ejecutadas para satisfacer los objetivos de la empresa.
- ***Chief Information Security Officer* (CISO).** Se trata de uno de los últimos perfiles que se han creado como director de seguridad de la información y que responde a la necesidad por parte de las empresas de contar con un experto en ciberseguridad que realice las funciones de monitorización y análisis de riesgos a los que se enfrentan en su día a día, garantizando la protección de la información mediante las medidas y los controles necesarios. El CISO está al cargo de la detección y el análisis de los puntos débiles de la empresa, además del manejo del control del acceso a la información de la compañía. Además de velar por la seguridad, también tiene que saber responder a posibles incidentes para que la operatividad de la empresa no se vea afectada
- **Delegado de protección de datos (DPO).** Se trata de un perfil que se encarga de preservar el cumplimiento normativo y que, a partir de la nueva ley europea de protección de datos GDPR, ha pasado a ser obligatorio en la Administración y en muchas empresas privadas, situándose en un puesto intermedio entre la dirección y la gerencia de la compañía. Es el responsable de informar y asesorar a todos los empleados de la organización sobre las obligaciones a que están sujetos por la normativa, además de supervisar su cumplimiento y actuar como punto de contacto con la autoridad competente.

Los perfiles anteriores tienen principalmente funciones ejecutivas y de tomas de decisiones y por debajo de ellos, más a nivel técnico, encontramos aquellos perfiles que se encargan

de ejecutar el plan de ciberseguridad tal y como se ha diseñado desde la dirección del área. Entre estos perfiles podemos destacar:

- **Arquitecto de ciberseguridad.** Es quien se encarga de llevar a cabo el plan de ciberseguridad a nivel técnico, construyendo la red a partir de las decisiones tomadas por la dirección, con el fin de garantizar la seguridad de todos los procedimientos que lleve a cabo la empresa. Se trata de un perfil esencial ya que se ocupa del diseño de la arquitectura de ciberseguridad y asegura que la estrategia de negocio y la seguridad de las tecnologías de la información están alineadas.
- **Ingeniero en ciberseguridad.** Los ingenieros en ciberseguridad se ocupan de la realización de pruebas de vulnerabilidades sobre los sistemas y del desarrollo de *scripts* de automatización que ayudarán a manejar y rastrear los incidentes. También son responsables de configurar, instalar y mantener los sistemas de seguridad y de detección de intrusiones.
- ***Incident responder.*** Es el responsable de investigar, analizar y responder a los ciberataques o incidentes de seguridad. Sin embargo, su posición no solo es reactiva, sino que también debe monitorizar de forma continua los sistemas y las redes para detectar intrusiones, realizar auditorías de seguridad y desarrollar planes de respuesta, así como conocer los planes de continuidad de negocio de la empresa si se produce un ataque exitoso. Una vez finalizado un ataque, quien ocupe esta posición se encarga de redactar un reporte acerca del incidente en el que se explique con cierto detalle cómo ocurrió el ataque y qué medidas se pueden adoptar para evitarlo en el futuro.
- **Analista forense y de *malware*.** Es el responsable de investigar los incidentes de seguridad relacionados con la recuperación de datos almacenados en dispositivos electrónicos y de reconstruir los sistemas dañados para recuperar datos perdidos. Sus principales funciones son el análisis de los sistemas de archivos, la adquisición de evidencias, el análisis de la memoria, la reconstrucción de ficheros, los métodos de infección y persistencia, la desinfección del *malware*, la ingeniería inversa o la criptografía.
- **Responsable de inteligencia.** Analiza y estudia las amenazas exteriores a la seguridad de la empresa.
- **Administrador de sistemas.** El administrador de sistemas es un perfil que muchas veces no se toma de forma estricta como profesional de la ciberseguridad. Sin embargo, es indispensable para la mayoría de las empresas, ya que es el responsable de la configuración, mantenimiento, operación y seguridad de los sistemas informáticos y servidores, así como de solucionar problemas y brindar apoyo a otros empleados.
- ***Pentester*, *penetration tester* o *hacker* ético.** También conocido como *hacker* de sombrero blanco, se ocupa de encontrar vulnerabilidades en los sistemas de las empresas con el objetivo de prevenir ataques externos. La labor principal de quienes se dedican a realizar pruebas de penetración es analizar sistemas y encontrar vulnerabilidades que puedan explotarse para obtener acceso a los sistemas informáticos. El *hacking* ético se

ha convertido en una práctica esencial para poner a prueba la seguridad de los servidores y sistemas de las empresas, simulando ataques para comprobar hasta qué punto una compañía está preparada o es vulnerable a los ciberataques.

- **Analista de ciberseguridad.** Se trata de un perfil cuyo objetivo es detectar las debilidades técnicas que puedan sufrir las empresas, encargándose de prevenir las amenazas a las que se enfrentan y protegerlas de posibles ataques. Analiza y testea los sistemas informáticos de la empresa para detectar posibles vulnerabilidades técnicas. Documenta las vulnerabilidades e informa tanto de forma interna como a clientes y colaboradores, para solucionar o minimizar los riesgos de seguridad.

El perfil de analista de ciberseguridad se trata de un perfil que puede compartir tareas con el *hacker* ético ya que su misión principal es detectar debilidades técnicas, lo que es más sencillo de encontrar si se pone a prueba el sistema. Hay un perfil dentro de los analistas que está todavía más especializado en la detección de posibles nuevas amenazadas, por lo que se le considera un experto en inteligencia de ciberseguridad.

1.3.2. GERENTE DE SEGURIDAD DE LA INFORMACIÓN

El nombre exacto de la persona que supervisa la seguridad de la información y la ciberseguridad varía de una organización a otra. Uno de los nombres más comunes es oficial de seguridad de la información (**CISO,** *Chief Information Security Officer*), aunque algunas organizaciones prefieren el término jefe de seguridad (**CSO,** *Chief Security Officer*) para denotar la responsabilidad de todos los asuntos de seguridad, tanto físicos como digitales.

Del mismo modo, las responsabilidades y la autoridad de los directores de seguridad de información suelen variar entre las organizaciones. En general, el gerente de ciberseguridad será responsable de:

- Desarrollar la estrategia de seguridad y proporcionar orientación estratégica.
- Verificar que los recursos de la organización se están utilizando de manera responsable.
- Supervisar el programa y las iniciativas de seguridad.
- Coordinarse con los propietarios de los procesos de negocio para mantener la alineación continua.
- Garantizar que se realicen las evaluaciones de riesgo e impacto al negocio.
- Desarrollar estrategias de mitigación de riesgo.
- Hacer cumplir las políticas y el cumplimiento normativo.
- Monitorizar la utilización de los recursos de seguridad.
- Gestionar incidentes de ciberseguridad y su resolución, así como incorporar las lecciones aprendidas dentro de la organización.

La actitud de la gerencia debe conducir a un gobierno eficaz de la seguridad y corresponde a la alta dirección establecer un ejemplo positivo en este sentido, ya que perfiles de niveles inferiores son más propensos a cumplir con las medidas de seguridad cuando ven que sus superiores siguen la misma línea de trabajo. El respaldo de la gerencia ejecutiva a los requisitos de seguridad hará que las expectativas de seguridad se cumplan en todos los niveles de la organización.



RECUERDA

Más allá de estos requisitos, el personal directivo y de toma de decisiones tiene la obligación de supervisar las actividades relacionadas con la ciberseguridad, así como la responsabilidad legal y ética de ejercer el debido cuidado en la protección de los activos clave de la organización, incluyendo su información confidencial y crítica.

1.3.3. GOBIERNO DE LA CIBERSEGURIDAD

De acuerdo con el modelo establecido por ISACA, la seguridad requiere la participación de los altos directivos de las empresas. El término que describe el compromiso de la alta dirección es el gobierno corporativo, que es el conjunto de responsabilidades y prácticas ejercidas por los responsables de una empresa (por ejemplo, el consejo y la alta dirección) con el objetivo de proporcionar dirección estratégica, asegurar que los objetivos sean alcanzados, garantizar que los riesgos sean gestionados adecuadamente, y verificar que los recursos de la empresa sean utilizados de manera responsable.

El objetivo de la seguridad de la información es desarrollar, implementar y administrar un programa de seguridad que alcance los siguientes cinco resultados básicos de un gobierno eficaz de seguridad:

- **Alineación estratégica:** alinear la seguridad de la información con la estrategia de negocio.
- **Administración de los riesgos:** ejecutar medidas apropiadas para mitigar los riesgos y reducir el posible impacto que tendrían en los activos de información.
- **Entrega de valor:** optimizar las inversiones en la seguridad.
- **Administración de recursos:** utilizar el conocimiento y la infraestructura de la seguridad de la información con eficiencia y eficacia.
- **Medición del desempeño:** es necesario monitorizar y reportar métricas de seguridad de la información para garantizar que se alcancen los objetivos.

Debido a que las organizaciones tienen diversas necesidades y sus enfoques de gobierno pueden variar, se ha identificado un conjunto básico de **principios y buenas prácticas** para ayudar a guiar estos esfuerzos entre los que podemos destacar:

- El riesgo de seguridad de la información es más que un problema de TI, es un componente clave en la gestión de riesgos de la organización, lo que requiere la supervisión de la dirección.
- El riesgo tiene implicaciones legales que los directivos deben entender.
- Los directores deben implementar un marco efectivo de gestión de riesgos en la organización.
- La alta dirección y el consejo deben evaluar el riesgo de seguridad de la información al igual que otros riesgos a nivel de organización para asegurar que los riesgos se acepten, eviten, mitiguen o transfieran.
- Realizar una evaluación anual de la seguridad de la información a cargo de la alta dirección.
- Llevar a cabo evaluaciones de riesgos periódicos como parte de un programa global de gestión de riesgos.
- Implementar políticas y procedimientos basados en las evaluaciones de riesgos.
- Establecer una estructura de gestión de seguridad para asignar individualmente roles y responsabilidades.
- Desarrollar iniciativas para brindar seguridad de la información a redes, instalaciones, sistemas e información en general.
- Tratar la seguridad de la información como parte integral durante el ciclo de vida de los sistemas de información.
- Proporcionar concienciación, capacitación y educación en seguridad de la información para todos los usuarios de la organización.
- Crear y ejecutar planes de acción para manejar cualquier deficiencia de seguridad de la información.
- Desarrollar e implementar procedimientos de respuesta a incidentes.
- Establecer planes, procedimientos y pruebas para proporcionar la continuidad de las operaciones.
- Utilizar las mejores prácticas de la industria, como la ISO 27001, o *frameworks* como NIST o CIS.

1.4. DOMINIOS DE LA CIBERSEGURIDAD

Tal y como se vio al introducir el concepto de ciberseguridad, mantener un cierto nivel de seguridad exige, efectivamente, un proceso continuo de mejora que incluya las siguientes fases: **análisis, prevención, detección y respuesta.** Estas etapas son complementarias entre sí y, realizadas adecuadamente, crean un círculo que permite mantener la seguridad a lo largo del tiempo.

La primera etapa, el **análisis de riesgos,** supone que el nivel de riesgo cambia con el tiempo ya que continuamente se descubren nuevas vulnerabilidades en los sistemas y también cambian las amenazas. Además, las empresas y organizaciones tampoco pueden mantenerse estáticas: cambian sus mercados, productos, servicios y objetivos. Todo ello hace que también cambien el impacto y la probabilidad y, por tanto, también lo hace el riesgo.

Las otras tres etapas son las que, realizadas de forma adecuada, permitirán detectar los intentos de intrusión y reaccionar ante ellos minimizando el impacto, al mismo tiempo que se aprende y se mejoran los mecanismos y procedimientos relacionados con la seguridad.

Los cuatro dominios de la ciberseguridad son:

- Conceptos de ciberseguridad.
- Principios de arquitectura de ciberseguridad.
- Seguridad de redes, sistemas, aplicaciones y datos.
- Respuesta a incidentes.

1.4.1. CONCEPTOS DE CIBERSEGURIDAD

Este dominio presenta una discusión sobre conceptos críticos, tales como:

- Gestión básica de riesgos.
- Vectores comunes de ataque y agentes de amenazas.
- Patrones y tipos de ataques.
- Tipos de políticas y procedimientos de seguridad.
- Procesos de control de ciberseguridad.

Se abordan todos estos conceptos en relación con cómo estos influyen en las políticas de seguridad y los procedimientos en materia de amenazas de ciberseguridad.

1.4.2. PRINCIPIOS DE ARQUITECTURA DE CIBERSEGURIDAD

Este dominio proporciona información que ayuda a los profesionales de la seguridad a identificar y aplicar los principios de la arquitectura de seguridad. En él se discute una variedad de tareas, incluyendo:

- Definir la arquitectura y la infraestructura comunes de seguridad y los marcos de trabajo.
- Definir la seguridad perimetral.
- Definir la topología del sistema y los conceptos sobre el perímetro de seguridad.
- Implementar cortafuegos (*firewalls*).
- Realizar un aislamiento y la segmentación de las redes.
- Definir métodos de monitorización, detección y registros de acceso.

Estas tareas se presentan poniendo especial atención en las mejores prácticas de seguridad y se discuten varios tipos de arquitecturas de seguridad con el objetivo de mostrar la importancia que tienen las capas de controles para lograr una defensa en profundidad.

1.4.3. SEGURIDAD DE REDES, SISTEMAS, APLICACIONES Y DATOS

Este dominio aborda técnicas básicas de bastionado de sistemas y medidas de seguridad, incluyendo las siguientes tareas:

- **Controles de procesos:**
  - Evaluaciones de riesgos.
  - Gestión de vulnerabilidades.
  - Pruebas de penetración en los sistemas.
- **Mejores prácticas para la seguridad de redes, sistemas, aplicaciones y datos:**
  - Amenazas y vulnerabilidades de seguridad en sistemas y aplicaciones.
  - Controles eficaces para la gestión de vulnerabilidades.

Estas tareas tienen como objetivo ayudar a los profesionales de la ciberseguridad a evaluar su tolerancia al riesgo y responder apropiadamente a las vulnerabilidades.

1.4.4. RESPUESTA A INCIDENTES

En este dominio se describen las medidas necesarias para responder ante un incidente de ciberseguridad, cubriendo las siguientes tareas:

- Definir categorías de incidentes de ciberseguridad.
- Definir los planes de recuperación de desastres y de continuidad del negocio.
- Definir los pasos de respuesta a incidentes.

Estas tareas tienen por objetivo proporcionar a los profesionales el nivel de conocimientos necesario para responder a incidentes de ciberseguridad.

1.4.5. DOMINIOS DE SEGURIDAD SEGÚN EL ESTÁNDAR ISO 27000

El estándar ISO 27000 describe la implementación de un sistema de administración de seguridad de la información completo e incluye todos los controles administrativos, técnicos y operativos para mantener la información segura dentro de una organización.

Este estándar define doce dominios de seguridad que representan los componentes del estándar ISO 27000 y sirven como base común para desarrollar estándares de seguridad organizativa y prácticas eficaces de administración de seguridad.

- **Evaluación de riesgos:** es el primer paso en el proceso de administración de riesgos. Determina el valor cuantitativo y cualitativo del riesgo relacionado con una situación específica o una amenaza reconocida.
- **Políticas de seguridad:** es un documento que aborda las restricciones y los comportamientos de los miembros de una organización y especifica a menudo cómo se puede acceder a los datos y quién puede acceder a determinados datos.
- **Organización de la seguridad informática:** es el modelo de gestión establecido por una organización para la seguridad de la información.
- **Administración de recursos:** es un inventario y el esquema de clasificación para los recursos de información.
- **Seguridad de los recursos humanos:** aborda los procedimientos de seguridad relacionados con los empleados que ingresan, se desplazan y dejan una organización.
- **Seguridad física y medioambiental:** describe la protección de las instalaciones informáticas dentro de una organización.
- **Administración de operaciones y comunicación:** describe la administración de los controles de seguridad técnica en los sistemas y las redes.
- **Adquisición, desarrollo y mantenimiento de los sistemas informáticos:** describe la integración de la seguridad en las aplicaciones.
- **Control de acceso:** describe la restricción de los derechos de acceso a las redes, los sistemas, las aplicaciones, las funciones y los datos.
- **Administración de incidentes de seguridad informática:** describe cómo anticipar y responder a las violaciones de seguridad informática.
- **Administración de la continuidad empresarial:** describe la protección, el mantenimiento y la recuperación de los sistemas y procesos críticos.
- **Cumplimiento:** describe el proceso de garantizar el cumplimiento de las políticas, los estándares y las regulaciones de seguridad informática.

1.5. GESTIÓN DE RIESGOS Y CONTROLES DE CIBERSEGURIDAD

La ciberseguridad juega un papel significativo en el panorama cibernético actual que está en constante evolución. Las nuevas tendencias en movilidad y conectividad presentan una amplia variedad de desafíos, puesto que los nuevos ataques continúan desarrollándose al mismo tiempo que las tecnologías emergentes.

Los profesionales de la ciberseguridad deben estar informados y deben ser flexibles para identificar y gestionar eficazmente nuevas amenazas potenciales, tales como las amenazas persistentes avanzadas (APT) que se consideran ataques de un adversario que posee

niveles sofisticados que permiten al atacante lograr sus objetivos utilizando múltiples vectores de ataque.

1.5.1. GESTIÓN DE RIESGOS

La protección de los activos contra las amenazas es una preocupación clave para la seguridad en general de las organizaciones. Además, la responsabilidad de proteger estos activos recae en las partes interesadas para quienes estos activos tienen valor. Por tanto, las partes interesadas deben tener en cuenta las amenazas al evaluar el riesgo a estos activos.

La gestión de riesgos es el proceso continuo de identificación, evaluación y respuesta al riesgo. Para administrar el riesgo, las organizaciones deben comprender la probabilidad de que ocurra un evento y el impacto resultante. Con esta información las organizaciones pueden determinar el nivel aceptable de riesgo para la prestación de servicios y pueden expresar esto como su tolerancia al riesgo.

Con una comprensión de la tolerancia al riesgo las organizaciones pueden priorizar las actividades de ciberseguridad, permitiéndoles tomar decisiones informadas sobre los gastos de esta. La implementación de programas de gestión de riesgos ofrece a las organizaciones la capacidad de cuantificar y comunicar los ajustes a sus programas de ciberseguridad.

Las organizaciones pueden optar por manejar el riesgo de diferentes maneras, incluida la mitigación, la transferencia, la prevención o la aceptación del riesgo, según el impacto potencial en la prestación de los servicios críticos.

El entorno empresarial, en particular, tiende a impulsar las decisiones sobre el riesgo. Por ejemplo, una pequeña empresa de nueva creación puede ser mucho más tolerante con el riesgo que una empresa grande y consolidada. Por tanto, puede ser útil hacer referencia a los criterios generales enumerados a continuación cuando se evalúan los factores que afectan a la seguridad de una organización específica.

RECUERDA

El **análisis de riesgos informáticos** es un proceso que comprende la identificación de activos informáticos y de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, es necesario poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta dicha organización mediante la aplicación de controles.

Estos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objeto de riesgo (u otras dimensiones requeridas para la organización como la trazabilidad).

1.5.2. CONTROLES DE CIBERSEGURIDAD

Los controles de ciberseguridad pueden clasificarse en función de su tipología:

- **Controles administrativos:** son aquellos controles procedimentales, administrativos o documentales que establecen las reglas a seguir para la protección del entorno. Tienen en cuenta aspectos como la documentación requerida para estandarizar la práctica de seguridad (como las políticas y los procedimientos), la formación y concienciación y el gobierno de la seguridad.
- **Controles lógicos:** son los controles basados en una combinación de *hardware* y *software* que tienen en cuenta aspectos como la protección de los servidores y de la red en general, la gestión de las identidades y el control de acceso.
- **Controles físicos:** son aquellos tipos de controles tangibles orientados a la protección del entorno y de los recursos físicos de la organización. Tienen en cuenta la protección contra accesos físicos no autorizados (puertas de seguridad, cámaras de vigilancia, sensores de movimiento, tornos), protección del equipamiento y contra amenazas medioambientales (protección contra incendios o inundaciones, protección contra vibraciones).
- **Controles preventivos:** son los controles que buscan evitar que un potencial atacante o amenaza pueda vulnerar el sistema. Ejemplos de esto serían los controles de acceso físicos y lógicos, los cortafuegos y los antivirus.
- **Controles de detección:** se trata de aquellos controles que buscan que, en caso de que una amenaza haya afectado a la organización, se pueda detectar de manera temprana con el objeto de minimizar el impacto a la organización. Ejemplos de esto serían los sensores físicos (agua, fuego) o los sistemas de monitorización de eventos de seguridad (SIEM).
- **Controles de recuperación:** en este caso buscarían recuperar la función de la organización en un tiempo que evite que el impacto ponga en peligro la viabilidad de la organización o que el perjuicio causado supere un umbral definido. Ejemplos de estos controles serían los planes de gestión de incidentes, las copias de seguridad, los planes de continuidad de negocio y la recuperación ante desastres.

Los controles anteriores se pueden materializar en seguir las mejores prácticas de ciberseguridad que pueden seguir las organizaciones, entre las que cabe destacar las siguientes:

- **Mantener un inventario de *software* autorizado y no autorizado:** tener visibilidad sobre el *software* en su red puede ayudar a identificar y eliminar el *software* prohibido, así como el riesgo de explotaciones de *software* desconocidas.
- **Mantener un inventario de *hardware* autorizado y no autorizado:** mantener y proteger los dispositivos de red remotos, ya sean computadoras portátiles o dispositivos móviles, puede ser un desafío, pero nunca debe descuidarse, ya que cada dispositivo es otra oportunidad para que un atacante pueda colarse.
- **Asegurar las configuraciones de *hardware* y *software:*** las configuraciones personalizadas para *hardware* y *software* pueden ayudar a mitigar los ataques de *hardware* y *software* específicos.
- **Seguimiento y control de cuentas:** a menudo, las cuentas de usuario caducadas no se eliminan de los directorios, lo que significa que dejan un vacío en la seguridad de la empresa. Del mismo modo, las contraseñas que nunca caducan aumentan la vulnerabilidad de esa cuenta con el tiempo. Debemos estar al tanto de las brechas de seguridad monitorizando la actividad de la cuenta y controlando las políticas de contraseñas.
- **Asegurar las aplicaciones:** con un número cada vez mayor de ejecuciones remotas de código que explotan vulnerabilidades de día cero, la seguridad de las aplicaciones se ha convertido en un elemento vital en las listas de verificación de seguridad para muchas empresas. Especialmente con el costo de las multas que llegan a millones de dólares si las empresas no cumplen.
- **Configuración adecuada del sistema:** supone configurar el sistema para que se comporte exactamente como se espera. La base de la seguridad informática tiene dos vertientes: que el sistema ofrezca los servicios que de él se espera y que, por otra parte, no pueda ser utilizado para otros propósitos como obtener información no autorizada o atacar a terceros.
- **Instalar versiones recientes de *software:*** es recomendable instalar versiones recientes del *software*. Efectivamente, cuando se descubren nuevas vulnerabilidades, estas se corrigen en las versiones posteriores del *software*. Por tanto, las versiones antiguas suelen incluir más vulnerabilidades que las recientes. No obstante, cuando se añade nueva funcionalidad o se realizan cambios significativos en un sistema, es habitual que se introduzcan nuevas vulnerabilidades. Por este motivo, en los sistemas en los que se desee mantener un elevado nivel de seguridad conviene esperar un tiempo antes de desplegar versiones con cambios significativos.
- **Instalar los parches disponibles:** en muchos casos, cuando se descubren nuevas vulnerabilidades, estas se solucionan realizando pequeños cambios sobre las versiones recientes del *software*. Estos cambios reciben el nombre de parches y es recomendable instalarlos lo antes posible, pues una vez que se publica una vulnerabilidad se abre una ventana de tiempo en la que los sistemas tienen una elevada probabilidad de ser atacados.

- **Monitorización:** el objetivo de esta actividad es poder detectar los ataques que se produzcan para poder reaccionar a tiempo. En el mejor de los casos, las medidas preventivas serán suficientes para evitar que el ataque tenga éxito. Cuando no es así, la monitorización permitirá detectar y tratar la intrusión lo antes posible, limitando así el daño causado. Esta actividad presenta, además, ventajas adicionales, ya que permite detectar todo tipo de situación anómalas, como sistemas de ficheros que están cerca de llenarse, discos que están a punto de fallar, fallos de configuración de las aplicaciones, saturación de las redes, etcétera.
- **Tratamiento de vulnerabilidades:** se puede definir una vulnerabilidad como una debilidad en el sistema. Es decir, algún punto débil que, si alguien lo encuentra, puede ser usado para conseguir que el sistema se comporte de forma diferente a la esperada. Las vulnerabilidades pueden existir tanto en los procedimientos, como en el diseño y la implementación.
  - **Vulnerabilidades en los procedimientos:** son puntos débiles en los procedimientos (no necesariamente informáticos) que se utilizan en el trabajo (empresas, organizaciones) o en la vida personal. Por ejemplo, que el procedimiento en una empresa para recuperar una contraseña olvidada sea llamar por teléfono. Un atacante podría aprovechar este procedimiento para conseguir establecer una contraseña de su elección en una de las cuentas. El ataque será más o menos sencillo en función de detalles del procedimiento tales como si es necesario usar un teléfono corporativo o está permitido llamar desde cualquier número, si se conocen todos en la empresa, o si se solicita algún mecanismo de identificación adicional.
  - **Vulnerabilidades en el diseño:** son puntos débiles del diseño del sistema. Por ejemplo, un sistema puede estar diseñado para usar contraseñas de un máximo de 8 caracteres. En este caso el atacante puede aprovechar este hecho para tratar de adivinar la contraseña o para probar todas las contraseñas posibles (ataque por fuerza bruta). El ataque será más o menos sencillo en función de cómo se eligen las contraseñas (para tratar de adivinarlas) o de la velocidad con la que sea posible probar contraseñas (fuerza bruta).
  - **Vulnerabilidades en la implementación:** aparecen cuando los puntos débiles se deben a que la implementación no se ajusta al diseño. Por ejemplo, el diseño permite contraseñas de longitud arbitraria, pero la implementación solamente almacena los primeros 8 caracteres, bien por limitaciones de los componentes utilizados, bien por un fallo de implementación.
- **Amenazas:** se puede definir una amenaza como el conjunto de circunstancias que puede causar un comportamiento no deseado del sistema. Las amenazas son peligrosas en tanto en cuanto existen puntos débiles (vulnerabilidades) que permiten que se produzca el daño (comportamiento no esperado del sistema). Los dos principales tipos de amenazas son las internas y las externas.

- Las **amenazas internas** se deben a personal interno o a posibles ataques lanzados desde dentro de la organización. Estas personas disponen de conocimiento del funcionamiento interno de los sistemas y, muchas veces, de acceso autorizado al sistema. También pertenecen a este grupo las amenazas de posibles ataques que se lancen desde dentro de la empresa.
- Las **amenazas externas** se corresponden con posibles ataques lanzados desde fuera de la empresa u organización. Evidentemente, ataques que inicialmente son externos pueden convertirse en internos en cuanto consiguen control de cualquier sistema corporativo, especialmente de aquellos menos protegidos.

1.6. *FRAMEWORKS* DE CIBERSEGURIDAD

Muchas organizaciones ya están siguiendo una arquitectura de seguridad, utilizando como base *frameworks* de seguridad entre los que podemos destacar:

- ***Framework* de ciberseguridad NIST:** *framework* de ciberseguridad del Instituto Nacional de Estándares y Tecnología de Estados Unidos (https://www.nist.gov/cyberframework).
- **CIS Controls:** define un conjunto de buenas prácticas específicamente dirigidas a detener los ciberataques (https://www.cisecurity.org/controls).

El propósito de estos *frameworks* es proporcionar una guía para la organización en la gestión de riesgos de seguridad de la información. Otro factor importante es proporcionar orientación para desplegar un sistema integrado para toda la organización del programa para la gestión de riesgos de seguridad de la información.

1.6.1. *FRAMEWORK* DE CIBERSEGURIDAD NIST

El *framework* de ciberseguridad de NIST (https://www.nist.gov/cyberframework/framework) consiste en estándares, líneas base y mejores prácticas para manejar los riesgos asociados a la ciberseguridad en una organización. Está diseñado para que sea flexible y eficiente en términos de costo, para promover la protección y resiliencia de infraestructura crítica en organizaciones gubernamentales o privadas.

El *framework* NIST utiliza procesos de gestión de riesgos para permitir que las organizaciones informen y prioricen las decisiones relacionadas con la ciberseguridad, dando a las organizaciones la capacidad de seleccionar y dirigir mejoras dinámicas en la gestión de riesgos de ciberseguridad para los entornos de TI.

Se trata de una guía basada en estándares, directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen mejor y reduzcan el riesgo de ciberseguridad. Además, su diseño está basado en fomentar las comunicaciones de gestión del riesgo y la ciberseguridad entre los usuarios internos y externos de la organización.

Los **objetivos** de este *framework* de ciberseguridad se podrían catalogar en los siguientes puntos:

- Describir el estado objetivo de la ciberseguridad.
- Identificar y priorizar oportunidades de mejora en el contexto de la ciberseguridad.
- Comunicación entre las partes interesadas internas y externas sobre los riesgos de ciberseguridad en las organizaciones.

El *framework* NIST consta de tres **componentes principales:**

1. **Núcleo:** conjunto de actividades y resultados deseados organizados en funciones, categorías y subcategorías.
2. **Niveles:** grado en el que la gestión de riesgos de la ciberseguridad adopta los controles definidos en el *framework*.
3. **Perfiles:** es la configuración de requisitos, objetivos, tolerancia al riesgo y recursos actuales respecto a los resultados deseados del *framework*.

El *framework* consta de cinco **etapas o funciones** que proporcionan una visión estratégica de alto nivel del ciclo de vida de la administración de riesgos de ciberseguridad de una organización.

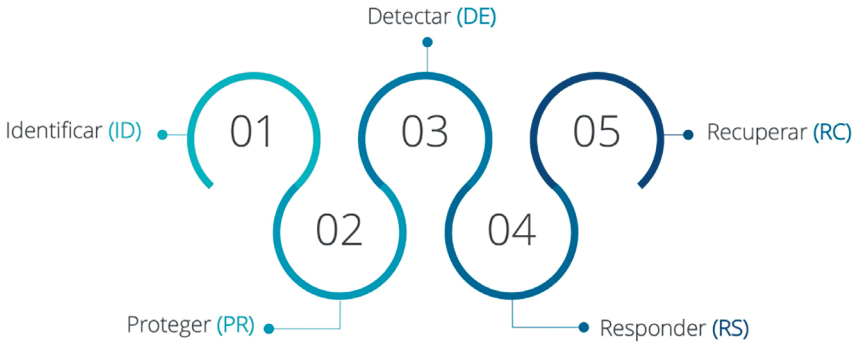


Figura 1.4. Etapas del ciclo de vida de la administración de riesgos de ciberseguridad.

Estas funciones se pueden realizar para formar una cultura operativa que aborde la problemática de los riesgos en ciberseguridad.

1. **Identificar.** En la primera etapa se establecen los riesgos potenciales y se realiza un inventario de los equipos, programas, datos y dispositivos que está utilizando la organización. A partir de esta información podríamos diseñar e implementar las diferentes políticas de ciberseguridad. En esta fase podríamos contemplar diferentes acciones, entre las que podemos destacar:
   a) **Gestión de activos.**
   b) **Ambiente de negocios.**

c) **Gobernanza.**

d) **Evaluación de riesgos.**

e) **Estrategia de gestión de riesgos.**

f) **Gestión del riesgo de la cadena de suministro.**

El objetivo de esta etapa es determinar los sistemas, activos, datos y competencias de la organización, su contexto de negocio, los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan a este entorno.

Las actividades en esta etapa son fundamentales para el uso efectivo del *framework* ya que permiten comprender el contexto, los recursos que respaldan las funciones críticas y los riesgos de ciberseguridad relacionados que permiten a una organización priorizar sus esfuerzos de acuerdo con una estrategia de gestión de riesgos.

2. **Proteger.** Esta etapa incluye la puesta en marcha de medidas de control de acceso a las redes y los dispositivos, el uso de programas de protección, la codificación de los datos almacenados y en tránsito, la realización de copias de seguridad, la definición de protocolos seguros para eliminar archivos y equipos, así como la formación de todas las personas vinculadas con la actividad.

   La función de protección admite la capacidad de limitar o contener el impacto de un posible evento de ciberseguridad. En esta fase podríamos contemplar diferentes acciones:

   a) **Gestión de identidad, autenticación y control de acceso.**

   b) **Conciencia y capacitación.**

   c) **Seguridad de los datos.**

   d) **Procesos de protección de la información.**

   e) **Mantenimiento.**

   f) **Tecnologías de protección.**

   El objetivo de esta etapa es desarrollar e implementar las contramedidas y salvaguardas necesarias para limitar o contener el impacto de un evento potencial de ciberseguridad.

3. **Detectar.** Esta etapa permite monitorizar la red para determinar si personas no autorizadas están accediendo a la misma, así como a los dispositivos, a los datos o al *software* instalado en los equipos de la organización. La función de detección permite el descubrimiento oportuno de eventos de ciberseguridad. En esta fase podríamos contemplar diferentes acciones:

   a) **Anomalías y eventos de seguridad.**

   b) **Monitorización de seguridad.**

   c) **Procesos de detección de amenazas.**

   El objetivo de esta etapa es desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad a través de la monitorización continua de la red.