ÍNDICE

Sobre los autores 21
Introducción 29
Prólogo 33

Capítulo 1.
***Ransomware* con exfiltración de datos** 37
1. Caracterización del ataque 40
   1.1. ¿Cómo es un ataque de *ransomware*? 40
   1.2. Grupos activos y TTP 42
   1.3. RDP, el vector clásico que sigue vigente 43
   1.4. Impacto en la organización 44
2. Acciones preventivas 47
   2.1. Reducir la superficie expuesta 47
   2.2. Endurecer la identidad 48
   2.3. *Backups* inmutables y probados 49
   2.4. Detección activa 51
   2.5. Concienciación continua 52
3. Acciones correctivas: cuando el ataque ya está aquí 53
   3.1. Si el cifrado se está produciendo en este momento 54
   3.2. Si el cifrado ya se ha consumado 55
   3.3. Pasos posteriores tras el aislamiento 57
   3.4. La pregunta del rescate 58
4. Acciones postincidente 61
   4.1. Revisión *post mortem* 61
   4.2. Refuerzo de controles 61

4.3. Cumplimiento regulatorio 61
4.4. Auditoría de validación..... 62
5. Conclusiones..... 64

Capítulo 2.
Brecha de seguridad con exfiltración de datos..... 67
1. Caracterización de la brecha con exfiltración 70
1.1. ¿Qué se entiende por exfiltración? 70
1.2. Cadena del ataque 70
1.3. Quién está detrás 73
1.4. El vector creciente: *infostealers*..... 74
1.5. Marco regulatorio aplicable a la notificación 74
2. Medidas preventivas..... 75
2.1. Clasificación y protección del dato..... 75
2.2. *Data Loss Prevention* (DLP) 76
2.3. EDR, XDR y telemetría centralizada 77
2.4. UEBA y detección de comportamientos anómalos 78
2.5. *Threat hunting* proactivo 79
3. Respuesta cuando la brecha ya ha ocurrido 80
3.1. Triaje inicial y contención..... 80
3.2. Investigación forense y determinación del alcance 81
3.3. Notificación regulatoria..... 83
3.4. Comunicación a los afectados y a terceros 85
4. Acciones postincidente..... 85
4.1. *Lessons learned* y revisión de controles 85
4.2. Endurecimiento técnico..... 86
4.3. Validación con auditoría posterior 87
5. Conclusiones..... 87
Referencias y fuentes consultadas..... 89

Capítulo 3.
Uso de *software* pirata 91
1. Por qué el *software* pirata es un problema de seguridad 94
   1.1. La economía del *software* pirata como vector de ataque 94
   1.2. Familias de *malware* habitualmente empaquetadas 95
   1.3. La cadena de riesgo en el entorno corporativo 96
   1.4. El caso particular del *software* de diseño, ingeniería y desarrollo 97
2. Medidas preventivas en la organización 98
   2.1. Política formal de uso de *software* 98
   2.2. Control técnico: prevención de instalaciones no autorizadas 99
   2.3. Alternativas legítimas a precio razonable 100
   2.4. Concienciación específica 101
3. Cuando ya está instalado: respuesta y remediación 102
   3.1. Inventario y triaje 102
   3.2. Análisis forense si hay indicios de compromiso 103
   3.3. Remediación técnica 105
   3.4. Legalización y regularización 106
4. Acciones postincidente y mejora continua 107
   4.1. Revisión de la política 107
   4.2. Concienciación reforzada 107
   4.3. Auditoría periódica 107
5. Conclusiones 108
   Referencias y fuentes consultadas 109

Capítulo 4.
***Backups*: la última red de seguridad** 111
1. Principios del *backup* moderno 113
   1.1. La regla 3-2-1 y su evolución 113

1.2. RTO y RPO: las dos métricas que importan 115
1.3. Inmutabilidad: por qué importa tanto 115
2. Errores frecuentes que conviene evitar 116
El caso típico que se observa en respuesta a incidentes 118
3. Procedimiento de recuperación 118
3.1. Recuperación tras *ransomware* 118
3.2. Recuperación tras fallo de *hardware* 119
3.3. Recuperación tras error humano o *malware* no destructivo 120
4. Pruebas, métricas y mejora continua 122
4.1. Niveles de prueba 122
4.2. Plan de Continuidad de Negocio y DRP 122
4.3. Métricas que conviene seguir 123
5. Conclusiones 123
Referencias y fuentes consultadas 124

Capítulo 5.
Denegación de servicio (DoS y DDoS) 127
1. Caracterización del ataque 130
1.1. DoS y DDoS: la diferencia que importa 130
1.2. Vectores por capa OSI 130
1.3. El factor IoT: por qué las *botnets* tienen tanta capacidad 132
1.4. Quién y por qué 132
2. Medidas preventivas 134
2.1. Servicios de mitigación *cloud* 134
2.2. Modelos de despliegue 136
2.3. Defensa de capa de aplicación 138
2.4. Endurecimiento de la infraestructura propia 139
3. Respuesta durante un ataque 139
3.1. Detección y triaje 140

3.2. Mitigación activa 140
3.3. La cuestión del pago en *ransom* DDoS 141
3.4. Notificación regulatoria 141
4. Después del ataque 142
5. Conclusiones 142
Referencias y fuentes consultadas 144

Capítulo 6.
***Phishing*, ingeniería social y suplantación de identidad en el correo electrónico** 145
1. Modalidades del ataque 148
1.1. *Phishing* genérico vs. dirigido 148
1.2. *Business Email Compromise* (BEC) 148
1.3. *Smishing, vishing* y *quishing* 150
1.4. AiTM y el factor MFA 151
1.5. El factor IA en el *phishing* moderno 152
2. Medidas defensivas 153
2.1. Autenticación del correo entrante (SPF, DKIM, DMARC) ... 153
2.2. Pasarela de correo segura 154
2.3. MFA resistente al *phishing* 155
2.4. Concienciación y *phishing* simulado 156
2.5. Controles específicos contra BEC 158
3. Respuesta tras un incidente de *phishing* 158
3.1. *Phishing* de credenciales 159
3.2. BEC con transferencia ejecutada 159
3.3. Cumplimiento regulatorio 160
4. Conclusiones 160
Referencias y fuentes consultadas 162

Capítulo 7.
***Hacking* de contraseñas** 165
1. Cómo se atacan las contraseñas 168
   1.1. Ataque por fuerza bruta 168
   1.2. Ataque por diccionario 169
   1.3. *Credential stuffing* y *password spraying* 170
   1.4. Ataques específicos contra *Active Directory* 171
   1.5. La realidad del ecosistema: *infostealers* y mercados 172
2. Políticas modernas de contraseñas 172
   2.1. El cambio de paradigma de NIST SP 800-63B 172
   2.2. Gestores de contraseñas 174
   2.3. MFA: imprescindible, no opcional 175
   2.4. Cuentas privilegiadas: PAM 176
3. El horizonte *passwordless* 178
   3.1. *Passkeys* 178
   3.2. SSO con identidad federada 178
4. Respuesta tras un compromiso de credenciales 179
5. Conclusiones 180
   Referencias y fuentes consultadas 182

Capítulo 8.
Ataques de fuerza bruta y de diccionario 185
1. Caracterización del ataque 187
   1.1. Fuerza bruta y diccionario 187
   1.2. Online frente a *offline* 188
   1.3. Servicios habitualmente atacados 189
   1.4. Herramientas y técnicas del atacante 189
   1.5. *Credential stuffing* y *password spraying* en detalle 191
2. Acciones preventivas 192
   2.1. Reducción de la superficie de ataque 192

2.2. Política moderna de contraseñas 193
2.3. MFA: el punto de inflexión 194
2.4. *Rate limiting*, bloqueo y *challenges* 194
2.5. Detección y monitorización 195
3. Respuesta ante un ataque en curso o exitoso 197
3.1. Si el ataque está en curso, pero no ha tenido éxito 197
3.2. Si el ataque ha tenido éxito 197
3.3. Análisis forense digital 198
4. Acciones postincidente 199
5. Conclusiones 199
Referencias y fuentes consultadas 201

Capítulo 9.
Ataques *man-in-the-middle* (*software* y *hardware*) 203
1. Caracterización del ataque 205
1.1. Qué es un ataque MITM 205
1.2. Variantes a nivel de *software* 206
1.3. Variantes a nivel de *hardware* (*wifi*) 207
1.4. Por qué la movilidad es el escenario más frecuente 208
2. Acciones preventivas 209
2.1. Inventario y arquitectura de red corporativa 210
2.2. *Wifi* corporativa: WPA3-Enterprise con 802.1X 210
2.3. Defensa criptográfica a nivel de aplicación 211
2.4. VPN o ZTNA siempre en movilidad 212
2.5. Disciplina del usuario en movilidad 213
3. Respuesta a un incidente MITM 215
3.1. Detección 215
3.2. Acciones inmediatas 215
3.3. Notificación regulatoria 216

4. Conclusiones 216
Referencias y fuentes consultadas 217

Capítulo 10.
Dispositivos infectados (USB, microSD y otros medios extraíbles) 219
1. Caracterización del ataque 221
1.1. Qué entendemos por dispositivo infectado 221
1.2. Taxonomía de ataques a través de USB 222
1.3. La familia Hak5 y la comercialización del ataque físico 224
1.4. Por qué sigue siendo eficaz 224
2. Acciones preventivas 226
2.1. Política escrita de medios extraíbles 226
2.2. Controles técnicos en el *endpoint* 227
2.3. Quioscos de escaneo previo 227
2.4. Detección y monitorización 228
2.5. Seguridad física y arquitectura 229
3. Respuesta ante un incidente 230
3.1. Detección de un dispositivo sospechoso 230
3.2. Acciones inmediatas 230
3.3. Notificación y registro 231
4. Conclusiones 231
Referencias y fuentes consultadas 232

Capítulo 11.
Redes *wifi* públicas y trabajo en movilidad 235
1. Caracterización del entorno 237
1.1. Qué es una red *wifi* pública 237

1.2. Riesgos típicos en *wifi* pública 238
1.3. Por qué la *wifi* pública sigue siendo un problema 239
2. Acciones preventivas 241
2.1. Política clara de uso de *wifi* pública 241
2.2. VPN o ZTNA con activación transparente 243
2.3. Endurecimiento del dispositivo en movilidad 243
2.4. Olvidar redes y desactivar conexión automática 244
2.5. Concienciación con escenarios reales 245
3. Respuesta a un incidente en movilidad 245
3.1. Sospecha de compromiso 245
3.2. Acciones inmediatas 246
4. Conclusiones 246
Referencias y fuentes consultadas 247

Capítulo 12.
Amenazas internas (*insiders*) 249
1. Caracterización del riesgo 252
1.1. Qué es un *insider* 252
1.2. Taxonomía operativa 252
1.3. Indicadores de comportamiento de riesgo 254
1.4. El factor del proveedor y la cadena de suministro 254
2. Acciones preventivas 255
2.1. *Onboarding* y cultura 255
2.2. IAM con *least privilege* 256
2.3. PAM y bóveda de credenciales 257
2.4. DLP y control de exfiltración 257
2.5. UEBA y detección de comportamiento 258
2.6. *Offboarding* riguroso 258
3. Respuesta a un incidente de *insider* 260

3.1. Triaje inicial 260
3.2. Contención sin alertar 260
3.3. Acción disciplinaria y legal 261
4. Conclusiones 261
Referencias y fuentes consultadas 262

Capítulo 13.
Dispositivos de ataque físico (Hak5 y similares) 265
1. Caracterización del riesgo 267
1.1. Qué entendemos por dispositivos de ataque físico 267
1.2. Catálogo de dispositivos relevantes 268
1.3. Vías típicas de introducción 270
2. Acciones preventivas 271
2.1. Control de acceso físico 271
2.2. Política de visitas y acompañamiento 272
2.3. Endurecimiento contra USB/HID 273
2.4. Network Access Control (NAC) y 802.1X cableado 273
2.5. Defensa frente a cables y periféricos troyanizados 274
2.6. Concienciación específica 275
3. Respuesta ante un incidente 277
3.1. Hallazgo de un dispositivo sospechoso 277
3.2. Detección de dispositivo en infraestructura 277
3.3. Notificación 278
4. Conclusiones 278
Referencias y fuentes consultadas 279

Capítulo 14.
Secuestro de correo electrónico y *Business Email Compromise* (BEC) 281
1. Caracterización del ataque 283
1.1. EAC y BEC: dos conceptos relacionados pero distintos 283
1.2. Modalidades reconocidas por el FBI 284
1.3. Cómo se compromete la cuenta 285
1.4. La fase silenciosa del ataque 286
2. Acciones preventivas 288
2.1. MFA universal y resistente al *phishing* 288
2.2. Autenticación de correo: SPF, DKIM, DMARC 288
2.3. Protección avanzada del correo 289
2.4. Endurecimiento de procesos de pago 290
2.5. Detección y monitorización 291
3. Respuesta ante un incidente BEC 292
3.1. Si se detecta un EAC, pero el BEC no ha sucedido 292
3.2. Si el BEC se ha consumado 293
3.3. Acciones de recuperación 294
4. Conclusiones 295
Referencias y fuentes consultadas 296

Capítulo 15.
Secuestro de redes sociales corporativas 299
1. Caracterización del riesgo 301
1.1. Qué es un secuestro de cuenta de redes sociales 301
1.2. Vectores de compromiso 302
1.3. Suplantación de marca: el problema complementario 304
2. Acciones preventivas 305
2.1. Inventario completo de cuentas y accesos 305
2.2. Identidad y autenticación robustas 306

2.3. Restricciones de uso y gestión 306
2.4. Configuración específica de cada plataforma 307
2.5. Monitorización y detección 308
3. Respuesta a un incidente 309
3.1. Acciones inmediatas (primera hora) 309
3.2. Si la recuperación no funciona 310
3.3. Comunicación y notificación 311
3.4. Recuperación y acciones postincidente 312
4. Conclusiones 312
Referencias y fuentes consultadas 313

Capítulo 16.
Pérdida o robo de *smartphone* 315
1. Caracterización del incidente 317
1.1. Qué se pierde con el dispositivo 317
1.2. Categorías del incidente 318
1.3. Por qué la respuesta tiene que ser muy rápida 319
2. Acciones preventivas 321
2.1. Inventario y trazabilidad 321
2.2. MDM/UEM como infraestructura básica 321
2.3. Cifrado y bloqueo robusto 322
2.4. Localización y borrado remoto 323
2.5. Protección frente a SIM *swap* 323
3. Respuesta ante un incidente 324
3.1. Acciones en la primera hora 324
3.2. Acciones en las 24 horas siguientes 325
3.3. Acciones postincidente 326
4. Conclusiones 327
Referencias y fuentes consultadas 328

Capítulo 17.
Pérdida o robo de dispositivos de almacenamiento 329
1. Caracterización del incidente 331
1.1. Alcance del incidente 331
1.2. Tipos de pérdida 332
1.3. Por qué el crifrado lo cambia todo 333
2. Acciones preventivas 335
2.1. Inventario y clasificación 335
2.2. Cifrado de disco completo (FDE) obligatorio 335
2.3. USB y discos externos cifrados 336
2.4. Gestión de claves de cifrado 336
2.5. Bloqueo automático y comportamiento del usuario 337
2.6. Borrado seguro al final del ciclo de vida 338
3. Respuesta ante un incidente 338
3.1. Triaje inicial 338
3.2. Si el dispositivo estaba cifrado y bloqueado 339
3.3. Si el dispositivo no estaba cifrado o no se puede confirmar 340
3.4. Si el dispositivo es recuperado 342
4. Conclusiones 342
Referencias y fuentes consultadas 343

Capítulo 18.
Plan de prevención de pérdida de datos (DLP) 345
1. Caracterización del programa 347
1.1. Qué es DLP 347
1.2. Tres estados de los datos 348
1.3. Causas habituales de pérdida de datos 349
2. Acciones preventivas: programa integral 351
2.1. Inventario y descubrimiento de datos 351
2.2. Clasificación con niveles operativos 351

2.3. Etiquetado automatizado 352
2.4. Gobierno: roles y responsabilidades 353
2.5. Mínimo privilegio y accesos 353
2.6. Concienciación específica 354
2.7. DLP de *endpoint* 354
2.8. CASB y DLP de correo en *cloud* 355
2.9. DLP de red y respuesta 355
3. Modo monitor frente a modo *enforce* 357
4. Respuesta a incidentes DLP 357
5. Conclusiones 358
Referencias y fuentes consultadas 359

Capítulo 19.
Madurez de ciberseguridad de la empresa 361
1. Qué es madurez de ciberseguridad 363
1.1. Definición operativa 363
1.2. Por qué medir la madurez 364
2. Marcos de referencia para evaluar madurez 365
2.1. NIST Cybersecurity Framework 2.0 365
2.2. NIST CSF Tiers: niveles de madurez 365
2.3. C2M2: complemento operativo del NIST 366
2.4. Niveles del ENS español 367
2.5. ISO/IEC 27001:2022 y el SGSI 368
3. Cómo evaluar la madurez en la práctica 368
3.1. Evaluación inicial 368
3.2. Indicadores clave (KPI y KRI) 369
3.3. Informes a dirección 369
4. Hoja de ruta de madurez 370
4.1. Fase 1: ganancias rápidas 370

4.2. Fase 2: capas operativas 371
4.3. Fase 3: capacidades proactivas 371
4.4. Plan director plurianual 373
5. Cumplimiento regulatorio y madurez 373
5.1. NIS2 y la madurez requerida 373
5.2. DORA para entidades financieras 374
5.3. ENS para sector público 374
5.4. RGPD transversal 374

Cierre del libro 375
Referencias y fuentes consultadas 378

Anexo.
Glosario consolidado 379