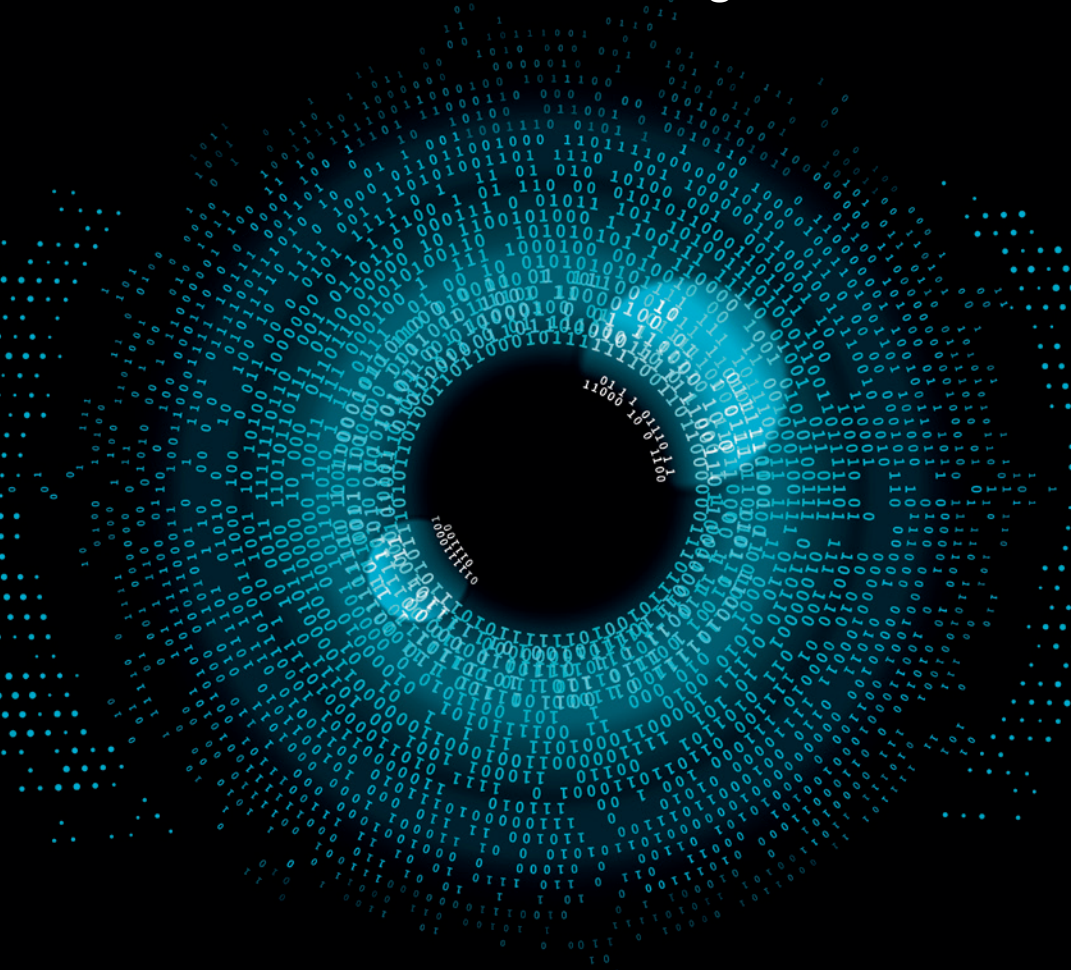


CIBERSEGURIDAD PASO A PASO

Diseña tu estrategia



MARÍA ÁNGELES CABALLERO
LAURA BAUS LERMA
DIEGO CILLEROS SERRANO

Índice de contenidos

Agradecimientos.....	6
Sobre los autores.....	7

INTRODUCCIÓN. UN NUEVO HORIZONTE DE AMENAZAS **19**

1. CIBERSEGURIDAD Y CÓMO CONSTRUIR TU ESTRATEGIA **25**

Vivimos en la nueva era digital	25
Tecnología exponencial e hiperconectada.....	26
Crecimiento exponencial tecnológico.....	26
Tecnologías exponenciales.....	27
Ley de Moore.....	28
Ley de los rendimientos acelerados.....	28
<i>Internet of Things</i>	29
Big Data.....	30
Inteligencia artificial.....	32
Tecnologías emergentes.....	32
Ciberdelincuencia, un problema de trillones de euros.....	34
¿Cómo de protegidas están las empresas?.....	36
¿Qué es un <i>hacker</i> ?.....	37
Filosofía <i>hacker</i> y argot.....	37
<i>White hat, sneaker</i> o <i>hacker</i> ético.....	39
<i>Black hats</i> o <i>crackers</i>	39
<i>Grey hats</i>	40
Conceptos básicos de ciberseguridad.....	40
Conceptos básicos de seguridad: CIA.....	40
Triángulo seguridad, funcionalidad y facilidad de uso.....	41
Perímetro de seguridad y malla de ciberseguridad.....	42

Zero Trust (cero confianza)	43
Defensa en profundidad o enfoque de seguridad por capas.....	43
Cómo construir tu estrategia de ciberseguridad	44
¿Qué es una estrategia de ciberseguridad?	44
¿Cuál es el objetivo de una estrategia de ciberseguridad?.....	44
¿Cómo construyo la estrategia de ciberseguridad para mi negocio? 4 pasos.....	45
Paso 1. Entiende tu entorno de amenazas	45
Paso 2. Evalúate a ti mismo: ¿dónde te encuentras?.....	46
Paso 3. Define tu plan de ciberseguridad: ¿dónde quieres estar?	47
Paso 4. Establece tu plan y evolucionalo: mirando al futuro	48
Macarena Bakes	49
Un mismo punto de partida	50

2. PASO 1. ENTIENDE TU ENTORNO DE AMENAZAS 51

Prepararse para la adversidad.....	51
Panorama actual de las ciberamenazas.....	52
Principales amenazas por sector.....	54
<i>Threat Actors</i>	55
Estado-nación	56
Cibercriminales.....	59
Hacktivistas.....	61
Grupos terroristas.....	62
Lobos solitarios	62
<i>Script kiddies</i>	63
Insiders.....	63
Amenazas de ciberseguridad.....	64
<i>Malware</i> y <i>ransomware</i>	65
<i>Phishing</i> e ingeniería social.....	75
Amenazas a los datos y filtraciones.....	85
<i>Distributed Denial of Service</i> o denegación de servicio distribuido.....	87
<i>Supply Chain Attack</i>	92
Errores, entrega incorrecta y mala configuración.....	97
Uso de credenciales robadas	99
<i>SIM Swapping</i>	102
<i>Cryptojacking</i>	106

3. PASO 2. DÓNDE TE ENCUENTRAS. EVALÚATE A TI MISMO CON CABACI 111

Por qué es importante evaluarse.....	111
¿Cómo nos vamos a evaluar? A través de un <i>Cybersecurity Framework</i> (CSF).....	112
Tipos de <i>Cybersecurity Frameworks</i>	113
Algunos ejemplos de CSF	114

<i>Framework CABACI</i>	115
Dominios.....	116
Controles y defensas.....	117
Controles básicos y avanzados	118
Controles.....	118
Controles para emprendedores	120
Defensas.....	121
Niveles de ciberseguridad.....	130
Define tu plan de ciberseguridad: AS-IS y TO-BE	131
Próximos pasos	132

4. PASO 2.1. ORGANIZACIÓN Y RIESGOS 133

Introducción	133
Defensas-Básicas.....	135
Control 1. Estrategia de negocio y organización.....	137
Defensa 1.1. Prioridades en la organización.....	137
Defensa 1.2. Organización de ciberseguridad.....	139
Defensa 1.3. Normativa de ciberseguridad.....	143
Control 2. Diseño tecnológico y gestión de activos.....	148
Defensa 2.1. Diseño tecnológico y de ciberseguridad	148
Defensa 2.2. Gestión de activos tecnológicos e inventario	150
Control 3. Gestiona tus ciberriesgos	153
Defensa 3.1. Identifica tus amenazas y riesgos.....	153
Defensa 3.2. Gestiona y prioriza tus riesgos	161
Defensa 3.3. Ciberseguro.....	162
Control 4. Seguridad en proveedores.....	164
Defensa 4.1. Identifica a tus proveedores tecnológicos.....	165
Defensa 4.2. Evaluación continua de la ciberseguridad de tus proveedores.....	167
Control C ² . Cultura cibersegura.....	171
Defensa C ² .1. Cultura cibersegura para empleados.....	171
Defensa C ² .2. Cultura cibersegura para <i>stakeholders</i>	174

5. PASO 2.2. PROTECCIÓN 177

Introducción	177
Protección de la red	187
<i>Firewalls</i>	187
<i>Firewalls</i> de última generación.....	189
Sistemas de detección/prevención de intrusos o IDS/IPS	190
VPN	191
<i>Network Traffic Analyzer</i> (NTA).....	192
NAC.....	193
SIEM.....	194
Seguridad wifi.....	194

Arquitecturas de seguridad.....	196	Defensa 7.4. Medidas <i>antispoofing</i>	246
ZTNA y SASE.....	199	Defensa 7.5. Cifrado y firma de correos electrónicos	247
<i>CyberSecurity Mesh Architecture</i> (CSMA).....	201	Control 17. Protección avanzada de dispositivos y sistemas	247
Protección de la red-Defensas	203	Defensa 17.1. Implementación de IDS/IPS local	247
Control 5. Protege tus redes wifi.....	204	Defensa 17.2. Guías de bastionado	248
Defensa 5.1. Segmentación de la red corporativa	204	Defensa 17.3. Gestión de privilegios.....	249
Defensa 5.2. Configuraciones seguras en redes inalámbricas.....	205	Defensa 17.4. Uso de <i>sandbox</i>	250
Defensa 5.3. Redes de invitados y políticas de uso.....	205	Protección de datos	251
Control 15. Protección avanzada de redes.....	206	Estrategias.....	253
Defensa 15.1. Arquitectura segura	206	Herramientas de seguridad	254
Defensa 15.2. Segmentación de redes	207	<i>Data-centric</i>	254
Defensa 15.3. Uso de <i>firewalls</i> de red.....	208	DAG	256
Defensa 15.4. Protección frente a intrusiones	209	DLP	256
Defensa 15.5. Protección de las conexiones remotas.....	209	IRM.....	258
Defensa 15.6. Uso de tecnologías avanzadas de protección de la red.....	210	DAM/DAF.....	258
Control 16. <i>Cloud</i> cibersegura.....	211	CASB.....	259
Defensa 16.1. Política de ciberseguridad <i>cloud</i>	211	Privacidad.....	261
Defensa 16.2. <i>Framework</i> de controles <i>cloud</i>	212	Las evaluaciones de impacto	264
Defensa 16.3. Protección de los datos y los repositorios <i>cloud</i>	212	El DPO	265
Defensa 16.4. Protección de entornos SaaS	213	El tratamiento de los datos.....	266
Defensa 16.5. Monitorización efectiva.....	214	Incidentes.....	267
Protección de sistemas y dispositivos de usuario	215	Protección de datos-Defensas	267
Seguridad física.....	216	Control 8. Protege tus datos.....	269
<i>Isolation</i> y <i>sandboxing</i>	216	Defensa 8.1. Protección de la información almacenada.....	269
Protección frente amenazas.....	217	Defensa 8.2. Prevención ante la pérdida o robo de información	269
Protección de las comunicaciones.....	219	Defensa 8.3. Gestión de claves de cifrado	270
Protección de la información	221	Defensa 8.4. Segregación de información sensible.....	271
Usuarios privilegiados locales.....	222	Defensa 8.5. Anonimización y pseudonimización de datos.....	272
Configuración segura de vulnerabilidades	223	Defensa 8.6. Cumplimiento de las regulaciones de privacidad	273
Gobierno y control	228	Protección de las aplicaciones.....	273
Protección del correo electrónico.....	230	OWASP Top 10.....	274
Amenazas y riesgos.....	231	Protección web.....	276
Capacidades de seguridad.....	234	CDN.....	276
Protección de sistemas y dispositivos de usuario-Defensas	237	WAF	277
Control 6. Protege tus dispositivos y sistemas	238	Denegaciones de servicio.....	278
Defensa 6.1. Política de uso responsable de dispositivos o sistemas	238	Seguridad en el desarrollo	279
Defensa 6.2. Control de inventariado y gestión de dispositivos	238	Seguridad en el diseño	280
Defensa 6.3. Control de <i>antimalware</i>	239	Gestión de accesos	282
Defensa 6.4. Implementación de <i>firewall</i> local.....	240	Análisis de dependencias	285
Defensa 6.5. Análisis de vulnerabilidades	241	Políticas de seguridad de contenido.....	286
Defensa 6.6. Parcheo de vulnerabilidades	242	Pruebas estáticas y dinámicas.....	287
Defensa 6.7. Protección de la navegación.....	242	Control de la integridad	289
Control 7. Protege tu correo electrónico.....	243	Protección de las aplicaciones-Defensas.....	290
Defensa 7.1. <i>Antispam</i> y <i>antiphishing</i>	243	Control 9. Protege tu página web.....	291
Defensa 7.2. Ejercicios de <i>phishing</i>	244	Defensa 9.1. Uso de <i>firewalls</i> de aplicaciones web (WAF).....	291
Defensa 7.3. Protección frente al <i>malware</i>	245	Defensa 9.2. Protección DDoS de las aplicaciones.....	292

Defensa 9.3. Uso de protocolos seguros en aplicaciones web.....	293
Defensa 9.4. Protección frente a <i>bots</i>	294
Defensa 9.5. Seguridad en APIs	294
Control 18. Desarrolla de manera segura.....	295
Defensa 18.1. Política de desarrollo seguro de software (S-SDLC) e implementación en terceros.....	295
Defensa 18.2. Cumplimiento de normas de desarrollo seguras	296
Defensa 18.3. Auditoría de código y pruebas de intrusión	298
Defensa 18.4. Gestión segura de las sesiones de usuario.....	298
Defensa 18.5. Verificación de dependencias y componentes de terceros	299
Defensa 18.6. Implementación de políticas de seguridad de contenidos (CSP).....	300
Protección de la identidad y el acceso	301
Gestión de identidades y control de accesos.....	302
Ciclo de vida de la identidad: alta/baja/modificaciones.....	304
Verificación, registro, autenticación, autorización y revocación	305
Autenticación multifactor.....	306
Gestión de cuentas privilegiadas	307
SSO (<i>Single Sign-On</i>).....	308
Federación de identidades	310
CIAM	311
Protección de la identidad y el acceso-Defensas	313
Control 10. Protege las credenciales de acceso.....	313
Defensa 10.1. Gestión del ciclo de vida de los usuarios.....	313
Defensa 10.2. Gestión de contraseñas robustas y rotación	314
Defensa 10.3. Uso de autenticación multifactor (MFA).....	315
Defensa 10.4. Gestión de permisos y privilegios	315
Control 19. Control de accesos avanzado	316
Defensa 19.1. Uso de sistemas de gestión de identidad y accesos (<i>Identity and Access Management Systems, IAM</i>)	316
Defensa 19.2. Segregación de funciones.....	317
Defensa 19.3. Gestión de cuentas privilegiadas	318
Defensa 19.4. Uso de <i>Single Sign-On</i> (SSO)	318
Defensa 19.5. Uso de la federación de identidades	319
Defensa 19.6. Uso de tecnologías CIAM (<i>Customer Identity and Access Management</i>).....	320
Protección de las redes sociales.....	322
Riesgos	323
Buenas prácticas.....	324
Protección de las redes sociales-Defensas.....	326
Control 11. Protege tus redes sociales.....	327
Defensa 11.1. Concienciación en protección de redes sociales.....	327
Defensa 11.2. Uso de credenciales robustas y autenticación de dos factores en redes sociales.....	328
Defensa 11.3. Configuraciones de seguridad y privacidad en redes sociales.....	329

Defensa 11.4. Seguimiento selectivo en redes sociales.....	330
Defensa 11.5. Prevención de <i>phishing</i> y fraude en redes sociales.....	331
Defensa 11.6. Prevención de <i>phishing</i> y fraude en redes sociales	332
Cultura cibersegura-Defensas	332
Defensa C ² .3. Cultura cibersegura sobre medidas de protección.....	333
Conclusiones para una estrategia en protección.....	334
Cómo implementar una estrategia en protección	334
Fase 1: <i>Quick wins</i>	335
Fase 2: Fundamentos de seguridad	335
Fase 3: Madurez en la ciberseguridad	336

6. PASO 2.3. DETECCIÓN, RESPUESTA Y RESILIENCIA 337

Más allá de la protección.....	337
Principales retos a los que nos enfrentamos	340
Mantener la calma en la crisis.....	341
Cyber Kill Chain.....	343
MITRE ATT&CK Framework	344
Cyber Kill Chain vs. MITRE ATT&CK Framework	344
Defensas-Básicas.....	345
Control 12. Responde a los ciberincidentes.....	347
Defensa 12.1. Plan de respuesta a incidentes actualizado	347
Defensa 12.2. Roles y responsabilidades en la respuesta	350
Defensa 12.3. Detección y evaluación del incidente	353
Defensa 12.4. Gestión y resolución del incidente.....	354
Defensa 12.5. Notificación del incidente	357
Control 13. Copias de seguridad	359
Defensa 13.1. Copias de seguridad.....	359
Control 14. <i>Feeds</i> de información y brechas de seguridad.....	360
Control 14. <i>Feeds</i> de información y brechas de seguridad	361
Defensas-Avanzadas	364
Control 20. Monitorización continua de ciberseguridad.....	365
Defensa 20.1. Define los activos tecnológicos a monitorizar	365
Defensa 20.2. Registra tus <i>logs</i>	367
Defensa 20.3. Establece la monitorización de tu red	370
Defensa 20.4. Monitorización continua de seguridad.....	372
Defensa 20.5. Gestión de eventos de ciberseguridad (SIEM)	375
Defensa 20.6. Security Operations Center.....	379
Control 21. Respuesta avanzada	384
Defensa 21.1. Capacitación de la respuesta	385
Defensa 21.2. Tecnología en la respuesta.....	387
Defensa 21.3. Ejecución de la respuesta a incidentes avanzada.....	390
Control 22. Gestión continua de vulnerabilidades	394
Defensa 22.1. Ciclo de vida de la gestión de vulnerabilidades	394

Control 23. Resiliencia	397
Control 23.1. Recuperación de incidentes.....	399
Control C ² . Cultura cibersegura.....	402
Defensa C ² .4. Ciberejercicios o simulacros de ataque.....	402

7. PASO 3. DEFINE TU PLAN DE CIBERSEGURIDAD 405

¿Dónde nos encontramos?	406
Define tu plan de ciberseguridad.....	408
AS-IS.....	408
Macarena Bakes. AS-IS	409
TO-BE.....	417
Macarena Bakes. TO BE.....	417
Macarena Bakes. Ejemplo de evaluación del dominio de Protección	426
Análisis inicial	427
Estado final.....	428
Fase 1: Quick Wins	429
Fase 2: Fundamentos de seguridad	429
Fase 3: Madurez en la ciberseguridad	430
Construyendo mi plan de ciberseguridad.....	431
Macarena Bakes. Construyendo mi plan de ciberseguridad	433
Dominio de Organización y riesgos.....	434
Dominio de Protección	435
Dominio de Detección, respuesta y resiliencia.....	437
Ya tenemos nuestro plan de ciberseguridad	438
Apetito de riesgo del negocio y "buy in".....	440
Apetito de riesgo del negocio: determinante para la estrategia de ciberseguridad	440
Planes de acción posibles cuando no se conoce el apetito de riesgo.....	442
Alinéate y mantén una escucha activa con tus <i>stakeholders</i>	443
Traduciendo plan y el riesgo en KRIs entendibles por negocio	445
Trabajemos el apetito de riesgo.....	448
Trabajemos los riesgos <i>cyber</i> -negocio.....	450
Representemos los riesgos <i>cyber</i> -negocio.....	450
Comuniquemos los riesgos <i>cyber</i> -negocio	453

8. PASO 4. ESTABLECE TU PLAN Y EVOLUCIÓNALO 457

Documentemos la estrategia.....	457
Definición de la estrategia y sus programas	459
Ciclo de vida del plan.....	461
Procedimientos y políticas <i>cyber</i>	462
Gobernemos la estrategia.....	463
Evolucionemos la estrategia	467

9. CIBERSEGURIDAD PARA EMPRENDEDORES 469

Introducción	469
Riesgos y amenazas específicas.....	470
Proteger su negocio	472
Sobre la organización y riesgos.....	473
Sobre la protección.....	476
Protege tus redes wifi	476
Protege tus dispositivos y sistemas.....	477
Protege tu correo electrónico.....	479
Protege tus datos	481
Protege tu página web	482
Protege las credenciales de acceso.....	485
Protege tus redes sociales	486
Sobre la detección, respuesta y resiliencia.....	487
Buenas prácticas en la actuación ante un ciberincidente.....	488
Concienciación	493
Mantener la privacidad personal y profesional	494

10. ESTRATEGIA DE CIBERSEGURIDAD EN CLOUD 495

Introducción	495
Los conceptos a conocer.....	499
Tipos de nube.....	499
Modelos de entrega	500
Responsabilidad compartida.....	504
Nube pública	507
Riesgos	507
Amazon Web Services (AWS).....	509
Infraestructura IaaS de AWS como aspecto básico	511
Seguridad de la nube y seguridad para la nube.....	516
Microsoft Azure	519
Infraestructura IaaS de Azure como aspecto básico	521
Seguridad de la nube y seguridad para la nube.....	524
Google Cloud Platform (GCP)	527
Estrategia de seguridad.....	530
Buenas prácticas de seguridad.....	531
<i>Framework</i> de controles y monitorización del cumplimiento.....	533
<i>Framework</i> CABACI	534
Certificación de servicios en nube	537
Protección de los datos en entornos SaaS.....	537

11. REGLAS DE ORO Y GUÍA DE CONTROLES CABACI 539

Y el final es solo el principio.....	539
Las reglas de oro	540
CABACI al completo	542
Organización y riesgos.....	543
Control 1. Estrategia de negocio y organización	543
Control 2. Diseño tecnológico y gestión de activos.....	544
Control 3. Gestiona tus ciberriesgos	545
Control 4. Seguridad en proveedores.....	546
Control C ² . Cultura cibersegura.....	547
Protección	549
Control 5. Protege tus redes wifi	549
Control 6. Protege tus dispositivos y sistemas	550
Control 7. Protege tu correo electrónico	555
Control 8. Protege tus datos	557
Control 9. Protege tu página web.....	561
Control 10. Protege las credenciales de acceso.....	563
Control 11. Protege tus redes sociales.....	565
Control 15. Protección avanzada de redes	568
Control 16. <i>Cloud</i> cibersegura.....	571
Control 17. Protección avanzada de dispositivos y sistemas.....	574
Control 18. Desarrolla de manera segura	576
Control 19. Control de accesos avanzado.....	579
Detección, respuesta y resiliencia	583
Control 12. Responde a los ciberincidentes	583
Control 13. Copias de seguridad	585
Control 14. <i>Feeds</i> de información y brechas de seguridad	586
Control 20. Monitorización continua de ciberseguridad.....	586
Control 21. Respuesta avanzada.....	589
Control 22. Gestión continua de vulnerabilidades	591
Control 23. Resiliencia.....	592

ÍNDICE ALFABÉTICO 593

Inteligencia artificial

Sin duda, una tecnología que está revolucionando el mercado y lo ha hecho en 2022 con el ChatGPT es la inteligencia artificial (IA). La IA es la capacidad de las máquinas para aprender datos y tomar decisiones por sí mismas. Sin duda, está cambiando el mundo. Por ejemplo, la IA está permitiendo mejorar el diagnóstico y tratamiento de pacientes, está ayudando a optimizar la producción manufacturera y mejorar la calidad de los productos reduciendo costes. Está permitiendo automatizar tareas peligrosas o repetitivas e incluso está haciendo tareas creativas como crear cuadros o música de una manera muy natural. Se espera que la IA tenga un impacto clave en la transformación de la movilidad con los vehículos autónomos y los sistemas de transporte inteligentes. También se espera ese impacto en la educación, permitiendo personalizar el aprendizaje y haciendo accesible la educación para todo el mundo. Estos son algunos ejemplos de muchos que podríamos nombrar. Lo cierto es que la IA con todo su potencial presenta varios riesgos de ciberseguridad.

Los ciberdelincuentes podrían tratar de manipular el código de una IA para que esta tomara decisiones erróneas o con mala intención. También podrían suplantar la identidad o engañar a través de técnicas de inteligencia artificial, de hecho, está pasando con los famosos *deep fakes*. Se puede utilizar para crear imágenes o información falsa y desinformar, es uno de los grandes problemas, el distinguir qué información es creada por un humano o es verídica y cuál es creada por máquinas. Finalmente, si la IA no se construye de una manera cibersegura y da fallos, puede perder fiabilidad y puede ser potencialmente explotable. La IA como tecnología exponencial está cambiando el mundo y su impacto será mayor en los próximos años, pero no nos podemos olvidar de la ciberseguridad que será clave en este viaje.

Tecnologías emergentes

Lo cierto es que la tecnología siempre ha existido y, durante generaciones y generaciones, el ser humano la ha ido evolucionando. En Atapuerca, en el Pleistoceno, que abarcó aproximadamente 2,6 millones de años hasta hace unos 11.700 años, se evolucionaba la tecnología como por ejemplo tener mejores armas para cazar y herramientas para alimentarse basadas en herramientas de hueso y marfil. Si nos vamos a la cita del capítulo, ya en la antigua Grecia, el propio Epitecto, filósofo estoico que vivió entre el 55 y 135 d. C., nos hablaba de tecnología. Por aquella época, las innovaciones tecnológicas incluían la construcción de edificios utilizando técnicas de arquitectura avanzada como columnas, arcos o bóvedas, construcción de carreteras, técnicas de navegación y cartografía o técnicas de producción de metales para producir

armas y herramientas. Hoy en día la tecnología sigue existiendo, pero se parece poco. Nuestras tecnologías son emergentes y convergentes, y tenemos tecnologías tan brillantes como la inteligencia artificial (IA), realidad aumentada o virtual (AR, VR), la ciencia de los datos o *data science*, biotecnología o *blockchain*. Se trata de innovaciones que permiten la mejora continua del ser humano, siempre y cuando se usen adecuadamente.

Vamos a ver tres de estas tecnologías emergentes que repuntarán en los próximos años:

- **Espacios inteligentes:** Espacios físicos o digitales que nos permiten interactuar con la tecnología, sistemas conectados, inteligentes, abiertos. Son cualquier área donde se instalan sensores para generar conocimientos de movimientos, dinámicas ambientales, actividades, personas o sistemas. Este conocimiento puede ser en tiempo real o históricos y se utilizan para mejorar las experiencias de las personas que usan ese espacio. Pueden ir desde espacios para actividades concretas hasta ciudades conectadas. Son espacios que utilizan la tecnología puntera a nuestro favor como IoT, realidad virtual y aumentada o la IA.
- **Inteligencia artificial generativa:** Técnicas de inteligencia artificial que aprenden de una representación a partir de datos y que utilizan estos datos para generar nuevos, originales y similares a los originales. Ya existen aplicaciones que están creando nuevos materiales como obras de arte. Solo 4 empresas de IA generativa recaudaron en 2022 alrededor de 370 millones de dólares en capital, empresas como Cresta, Adept AI, Stability AI y Jasper. ¿Pensábamos que la creatividad solo podría darse por los humanos? Solo tienes que mantener una conversación con ChatGPT (IA entrenada a base de texto) desarrollado por la empresa OpenAI para sorprenderte de lo que cambiará en los próximos años la manera de interactuar en el mundo.
- **El metaverso:** Esta "tecnología" o concepto amplía nuestro mundo físico, nuestras fronteras, a un mundo virtual totalmente nuevo, nuevas formas de relacionarnos entre los seres humanos. Las empresas de videojuegos y el propio Meta (antes Facebook) están invirtiendo bastante dinero en ello. El metaverso es un entorno digital e inmersivo interconectado que utilizará protocolos de comunicación que hoy día no se conocen. Se cree que será la evolución de Internet, aunque está en un estado muy latente. Es posible que las experiencias del metaverso desplacen a experiencias físicas que hoy conocemos y, de nuevo, los riesgos del mundo físico o digital se trasladarán al metaverso.

2

Paso 1. Entiende tu entorno de amenazas

"La suerte es lo que sucede cuando la preparación coincide con la oportunidad".

—Séneca

Prepararse para la adversidad

Estudiar las amenazas de ciberseguridad y prepararnos para enfrentarlas lo podemos ver como *premeditatio malorum* o preparación mental de los estoicos. En la filosofía estoica, se enfatiza la importancia de estar preparado para los desafíos que ocurren en la vida. Esto implica no solo prepararse para lo que se espera, sino para las incertidumbres que puedan surgir. Una organización que estudia y se prepara frente a las amenazas de ciberseguridad puede estar mejor preparada para salir victoriosa ante una ciberadversidad.

El primer paso, en la figura 2.1, para construir nuestra estrategia de ciberseguridad es **entender cuál es el entorno de amenazas de ciberseguridad** en el que se mueve su negocio y, para ello, a lo largo de este capítulo, nos adentraremos en profundidad sobre quiénes son los tipos malos, los actores de amenazas y cuáles son sus motivaciones, qué tipos de ataques existen como *ransomware*, *malware*, *supply chain* o *phishing*, a cuáles de ellos estamos más expuestos y con qué probabilidad e impacto.

Queremos que el libro sea práctico, así que veremos para cada actor de amenazas y para cada amenaza cómo le afectaría a Macarena Bakes, a nuestro negocio *e-commerce* de entrega de repostería *online*. Intentaremos hacer la vida de Macarena un poco más dulce y menos adversa!

- **Drive-by downloads:** Se trata de cualquier tipo de descarga de software malicioso que ocurre sin el conocimiento del usuario. Normalmente, la vía de propagación es mediante páginas web que contienen un *script* dentro del propio código HTML de la web. Si el usuario hace clic en la URL, se ejecutará este *script* e infectará su máquina con *spyware* o algún otro tipo de *malware*.
- **Rootkits:** Se trata de programas que pueden ejecutarse en un sistema durante un largo periodo de tiempo sin ser detectados. Se ejecutan a nivel de *root* o en el anillo 0 de los sistemas operativos. Cuando un *rootkit* es instalado en un sistema, puede ser controlado de manera remota sin que el usuario tenga conocimiento de ello. Aunque este *malware* es muy difícil de detectar por los programas antivirus, ya existen programas en el mercado para detección de *rootkits*, como por ejemplo la herramienta gratuita de Sophos, **Rootkit Removal**, que se puede encontrar en su página web: <http://www.sophos.com/en-us/products/free-tools/sophos-anti-rootkit.aspx>. Los sistemas operativos de Microsoft de 64 bits incluyen protección contra *rootkits*; hacen uso de **Kernel Patch Protection** o **Patchguard** que previene a los *rootkits* modificar los componentes del *kernel* del sistema operativo.

Nota: Las capas o anillos de seguridad, en la figura 2.9, hacen referencia a los mecanismos de protección de datos presentes en un fallo o comportamiento potencialmente malicioso. Gracias a esto, los sistemas operativos proporcionan diferentes niveles de seguridad de acceso a los recursos. Los niveles van desde el anillo 0 (*kernel*), anillo 1 y anillo 2 (controladores de dispositivos) y anillo 3 (aplicaciones). El nivel 0 es el nivel con mayores privilegios e interactúa directamente con el hardware, por ejemplo, la CPU (unidad central de proceso) o la memoria.

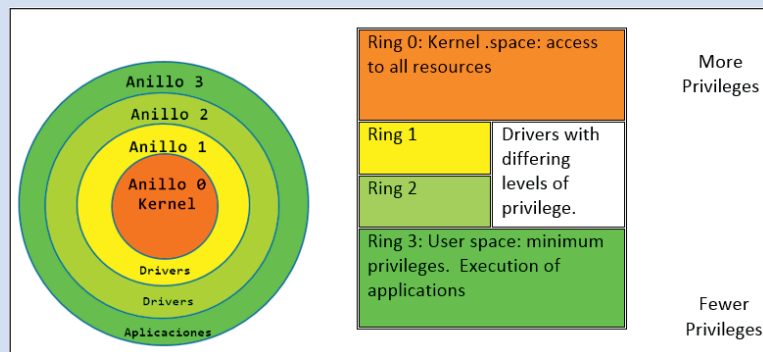


Figura 2.9. Arquitectura de anillos de seguridad con diferentes niveles de privilegios. Fuente: INCIBE.

- **Spyware y adware:** Se trata de un software que se puede instalar así mismo en la máquina de un usuario sin el conocimiento o consentimiento de este. Antiguamente, el *spyware* no se consideraba malicioso, ya que su propósito era intentar comprender la navegación del usuario o hábitos de compra para enviar publicidad a este. Hoy en día es considerado una forma de *malware* debido a que causa mucho más daño al sujeto. Muchas aplicaciones de *spyware* pueden identificar todos los sitios web que el usuario visita, todos los usuarios y contraseñas que utiliza, las teclas que pulsa, aunque no esté visitando un sitio web e incluso información clave del sistema como ficheros de usuarios y contraseñas u otros. El *spyware* puede llegar a cambiar determinadas configuraciones de la máquina, como deshabilitar el *firewall* o las actualizaciones automáticas. *Adware* es una variante del *spyware*, que muestra de manera intrusiva publicidad a un usuario en ventanas emergentes del navegador o *pop-ups* que son realmente molestos.
- **Keylogger:** Este término surge de la combinación de las palabras inglesas *key* (tecla) y *logger* (registro), y como su propio nombre indica registra las pulsaciones que se realizan en el teclado. Se trata de un tipo de *malware* que se instala en nuestro ordenador de manera malintencionada y sin que el usuario sea consciente de ello. El objetivo principal de este tipo de *malware* es el de hacerse con contraseñas de páginas web o cuentas bancarias para finalmente robar información o dinero a la víctima. Existen *keyloggers* tanto de tipo software como de tipo hardware.
- **Ransomware o Roguesoftware:** El *roguesoftware* o "virus de la policía" es un tipo de *malware* que simula ser una falsa aplicación del sistema para hacer creer a la víctima que tiene algún tipo de problema. Si la víctima quiere solucionar este supuesto problema, se le ofrece la posibilidad de pagar por ello. Curiosamente, en algunas ocasiones, si se abona la cantidad que el programa solicita, desaparece la infección. Los tipos de *roguesoftware* más extendidos son los que simulan ser un falso antivirus o un programa de la propia policía, de ahí su nombre, "virus de la policía". En este caso, el *malware* simula haber detectado contenido fraudulento como películas con contenido pornográfico o incluso pedófilo. Algunos de ellos simulan ser organizaciones como la Agencia Española de Protección de Datos (AEPD) y acusan a la víctima de almacenar contenido en su máquina que va contra la Ley Orgánica de Protección de Datos, Ley de Propiedad Intelectual o incluso contra el Código Penal español.

En el caso del falso antivirus, se hace creer al usuario que este antivirus ha realizado un escaneo de los archivos de su ordenador y ha encontrado la existencia de algún troyano en la máquina. Posteriormente, redirige a la víctima a una página con varios programas para desinfectar el ordenador, donde habrá que pagar por

Modus operandi

Habitualmente, la infección de estas máquinas se hace sin conocimiento del usuario y mediante algún tipo de *malware*. Algunas organizaciones hacktivistas, como Anonymus, han creado programas, como el famoso LOIC (Low Orbit Ion Canon), en la figura 2.15, y sus versiones (IRCLOIC, LOIQ, JSLOIC, etc.), para que los simpatizantes de esta organización se instalen este programa y se permita el uso de los recursos de sus máquinas para así lanzar ataques de DDoS contra las empresas u organizaciones que estos consideren. La aplicación envía una gran cantidad de paquetes TCP, UDP y peticiones HTTP para determinar la cantidad de conexiones por segundo que puede soportar la red objetivo hasta que quede fuera de juego. Es lo que se conoce como ataque por inundación o *flood*.



Figura 2.15. Programa LOIC, Low Orbit Ion Canon.

Tipos

Los ataques más habituales de DDoS son los **ataques por volumen** llamados "inundaciones". También se pueden dar **ataques de protocolo**, que tratan de enviar olas de paquetes desde ordenadores infectados con *malware* o *bots*, a determinados protocolos. Y, por último, se dan **ataques a aplicaciones** concretas, afectando a la capa 7 de la pila TCP/IP. Estos se basan menos en fuerza bruta y más en buscar vulnerabilidades concretas de las aplicaciones. Habitualmente, los ataques DDoS se pueden segregar según la capa OSI a la que están atacando, como se ve en la figura 2.16. Normalmente, los

ataques afectan a las siguientes capas: red (capa 3), transporte (capa 4), presentación (capa 6) y aplicación (capa 7). En la propia web de AWS podemos ver una tabla bastante descriptiva al respecto: <https://aws.amazon.com/es/shield/ddos-attack-protection/>.

Modelo de interconexión de sistemas abiertos (OSI):				
#	Capa	Aplicación	Descripción	Ejemplo de vector
7	Aplicación	Datos	Procesamiento de red para la aplicación	Inundaciones HTTP, inundaciones de consultas DNS
6	Presentación	Datos	Representación de datos y cifrado	Abuso de SSL
5	Sesión	Datos	Comunicación entre hosts	N/D
4	Transporte	Segmentos	Conexiones integrales y confiabilidad	Inundaciones SYN
3	Red	Paquetes	Determinación de la ruta y direccionamiento lógico	Ataques de reflexión UDP
2	Enlace de datos	Marcos	Direccionamiento físico	N/D
1	Físico	Bits	Medios, señal y transmisión binaria	N/D

Figura 2.16. Ataques DDoS por capa OSI. Fuente: AWS.

Veamos cuáles son los ataques DDoS más comunes:

- **SYN Flood o Inundación SYN:** El atacante suplanta la identidad o credenciales de un usuario legítimo para inundar los servidores con paquetes SYN, provocando que la red se colapse. Es un ataque difícil de realizar y en ocasiones los *firewalls* o sistemas anti-DDoS pueden detectarlo.
- **ICMP Flood o Inundación ICMP:** En lugar del envío de paquetes SYN, en este caso se hace envío masivo de paquetes ICMP para inundar la red. Esto provoca ralentización de los servidores que podría no solo ocupar el ancho de banda, sino dañar el sistema. También es un ataque difícil de realizar, dado que este tipo de tráfico suele estar limitado para evitar este tipo de ataques.
- **UDP Flood o Inundación UDP:** El protocolo UDP es el que manejan las aplicaciones que no utilizan paquetes de respuesta, dado que no pasa nada si estos se pierden, por ejemplo, aplicaciones de vídeo o transmisión constante de información. El atacante enviará paquetes UDP masivos para tratar de inundar los recursos de la red.
- **DNS Flood o Inundación DNS:** Los servidores DNS o servidores de nombre de dominio traducen las URL de las páginas web en direcciones IP. Por ejemplo, si queremos acceder a la web www.grupoanaya.es, como se ve en la figura 2.17, el servidor DNS traducirá la URL en la dirección IP 194.224.88.245. Si el atacante es capaz de inundar el servidor DNS, bloquearía el acceso a la web en cuestión.

Defensas: Organización y riesgos

En la figura 3.4, se presentan todas las defensas del dominio.

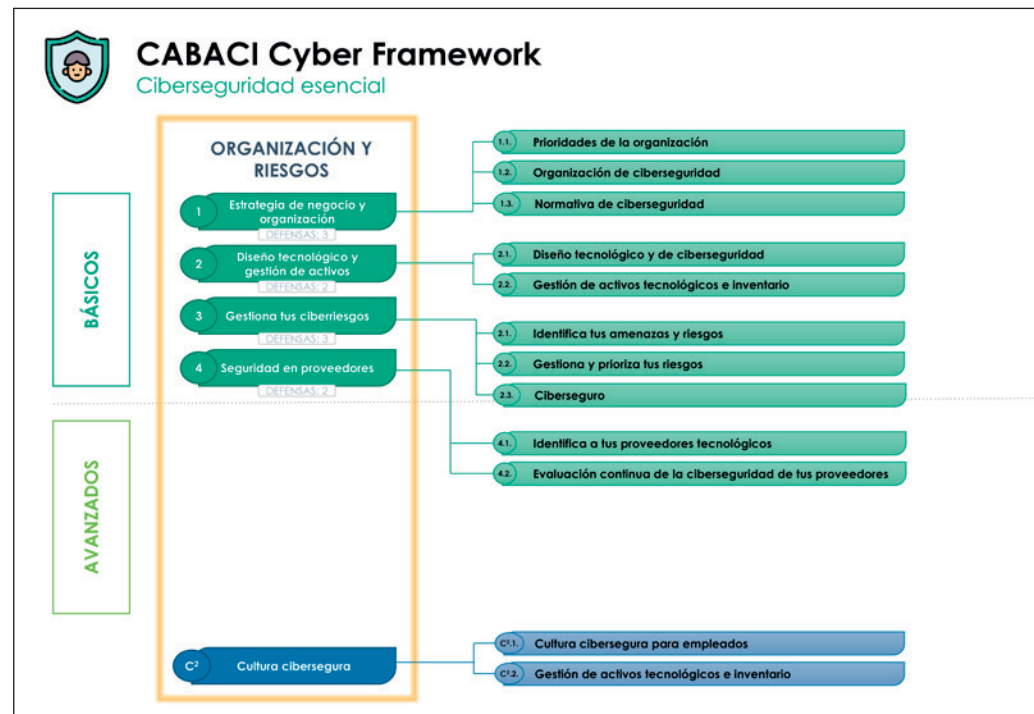


Figura 3.4. Framework CABACI-Defensas-Organización y riesgos.

Veamos las defensas de este dominio. Recordemos que solo tenemos defensas básicas en este dominio.

- Control 1. Estrategia de negocio y organización.
 - Defensa 1.1. Prioridades en la organización.
 - Defensa 1.2. Organización de ciberseguridad.
 - Defensa 1.3. Normativa de ciberseguridad.
- Control 2. Diseño tecnológico y gestión de activos.
 - Defensa 2.1. Diseño tecnológico y de ciberseguridad.
 - Defensa 2.2. Gestión de activos tecnológicos e inventario.

- Control 3. Gestiona tus ciberriesgos.
 - Defensa 3.1. Identifica tus amenazas y riesgos.
 - Defensa 3.2. Gestiona y prioriza tus riesgos.
 - Defensa 3.3. Ciberseguro.
- Control 4. Seguridad en proveedores.
 - Defensa 4.1. Identifica a tus proveedores tecnológicos.
 - Defensa 4.2. Evaluación continua de la ciberseguridad de tus proveedores.
- Control C². Cultura cibersegura.
 - Defensa C².1. Cultura cibersegura para empleados.
 - Defensa C².2. Cultura cibersegura para *stakeholders*.

Defensas: Protección

En las figuras 3.5 a la 3.7, se presentan todas las defensas del dominio.

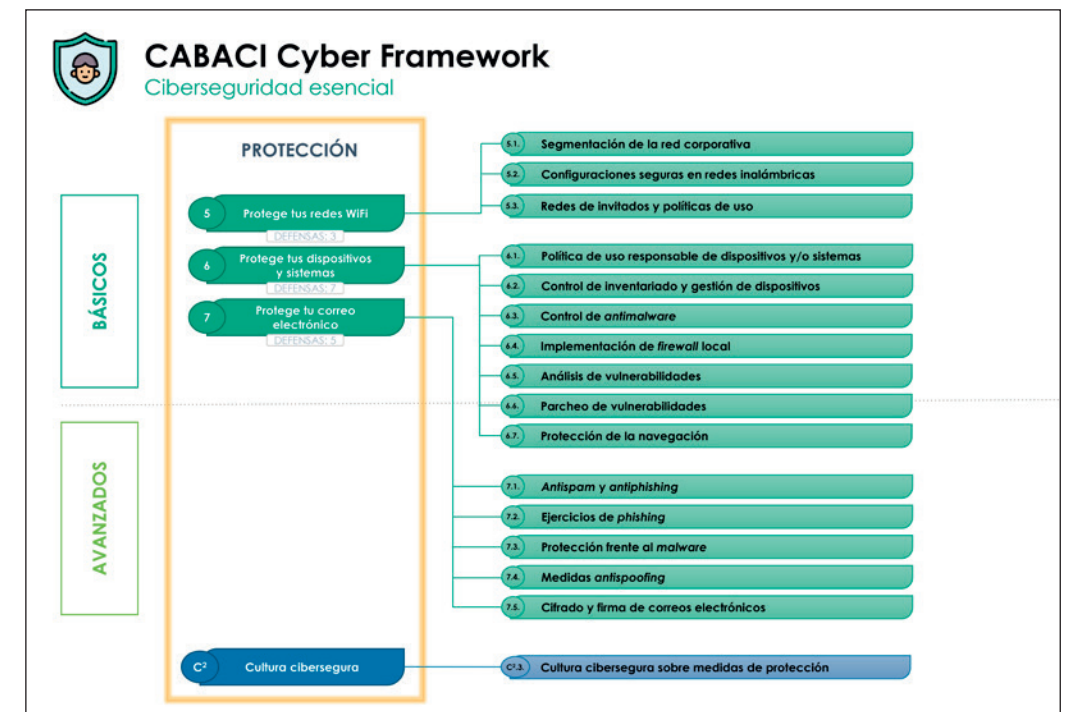


Figura 3.5. Framework CABACI-Defensas-PROTECCIÓN-Básicos 1.

dirección, para poder elevar los riesgos adecuadamente y que estos sean o mitigados o aceptados por los miembros del mismo o, al menos, que exista un comité de ciberseguridad en el cual el comité de dirección se encuentre representado.

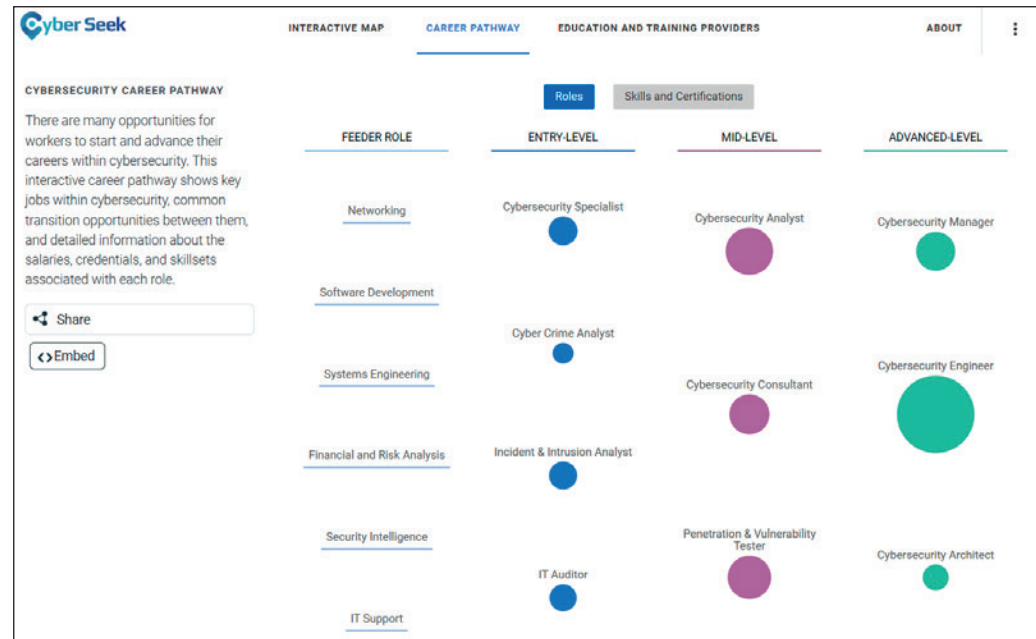


Figura 4.5. CyberSeek, <https://www.cyberseek.org/pathway.html>.

El CISO suele ser una posición de alto nivel que puede depender del CEO o director general de la organización o, al ser una posición directamente relacionada con tecnología, puede depender del CIO o director de tecnología, pero esta dependencia podría generar un conflicto de intereses, ya que el CIO velará habitualmente porque existan eficiencias tanto a nivel de tecnología y de costes y no tanto por la ciberseguridad y, además, querrá sacar proyectos adelante de manera rápida y con buena experiencia de usuario; por lo tanto, es importante que, en este caso, en las responsabilidades del CIO, también esté la ciberseguridad y que tenga fuerte conciencia de ciberseguridad.

CISO como un facilitador del negocio

Además, es clave que para ganar independencia y credibilidad el CISO adopte una actitud pragmática y sea una palanca tecnológica y de innovación. Se deben de establecer las reglas del juego mediante políticas y procedimiento de ciberseguridad, pero el CISO debe de ser un facilitador tanto del negocio como tecnológico, evaluando los riesgos constantemente según evolucionan ambos. Experiencia de usuario y ciberseguridad

deben ir de la mano. El mejor ejemplo funcional de esto es la detección de la huella o la cara para desbloquear nuestros teléfonos móviles. Se trata de una manera muy rápida de desbloquear el teléfono, por lo tanto, mejora la experiencia de usuario, pero a su vez, al involucrar biometría, es una manera de autenticarse segura.

Defensa 1.3. Normativa de ciberseguridad

- **Tipo de control:** Básico.
- **Madurez de mi control:** ¿Existe una normativa de ciberseguridad escrita, aprobada por la alta dirección y se ha diseminado en la organización?
- **Medición de la madurez:**
 - **Nivel 1. En riesgo:** No existe normativa de ciberseguridad escrita.
 - **Nivel 2. Incompleto:** Existe normativa de ciberseguridad escrita, pero es incompleta o no se conoce en la organización o no se ha aprobado por la alta dirección.
 - **Nivel 3. Adaptativo:** Existe una normativa de ciberseguridad escrita, aprobada por la alta dirección y se ha diseminado en la organización.

Es importante definir, escribir y diseminar normativa de ciberseguridad para toda la organización (políticas, estándares y procedimientos) y que esta venga avalada por la alta dirección de la compañía para conseguir que se implanten de manera efectiva.

Algunos de los motivos por los que es importante disponer de normativa de ciberseguridad son:

- Ayuda a la empresa a **proteger la confidencialidad, integridad y disponibilidad** de la información, sistemas y aplicaciones.
- Impulsa el **cumplimiento de normas y regulaciones** que nos puedan afectar de nuestro sector como puede ser normativa SOX, PCI-DSS o el RGPD.
- **Mitiga los riesgos de ciberseguridad** impulsando controles y tecnología para la protección de la organización.
- Sirve como vehículo para **concienciar**, principalmente a los empleados, fomenta el conocimiento en ciberseguridad de todos los empleados, apoyando una cultura cibersegura en la organización.
- A través de las medidas de ciberseguridad y la concienciación ayuda a proteger la **reputación de la organización**, así como a evitar posibles brechas de ciberseguridad, daños financieros, etc.

Una vez claro el "para qué" de la normativa de ciberseguridad, tenemos que ver cómo definimos, escribimos y formalizamos las políticas, estándares y procedimientos.

- **Protección de las aplicaciones:** Este subdominio se centraría en los controles para asegurar las aplicaciones que utiliza la organización. Esto podría incluir la revisión de seguridad del código, las pruebas de intrusión, la gestión de las configuraciones de seguridad de las aplicaciones y la protección contra ataques a nivel de aplicación como inyección SQL y *cross-site scripting* (XSS).
- **Protección de la identidad y el acceso:** Este subdominio se centraría en los controles para garantizar la seguridad de las identidades de usuario y la gestión del acceso a los sistemas y datos. Esto podría incluir la implementación de la autenticación multifactor, políticas de contraseñas seguras, control de acceso basado en roles o atributos, gestión de cuentas privilegiadas y monitorización y auditoría de eventos de acceso. La protección de la identidad y el acceso es fundamental para prevenir accesos no autorizados y minimizar el riesgo de brechas de seguridad.
- **Protección de las redes sociales:** Este subdominio está enfocado a establecer posibles controles y medidas de seguridad para proteger una herramienta más que las empresas utilizan como parte de su negocio y de su marca digital. No es el típico subdominio que se encuentre en un *framework* de ciberseguridad, pero creemos que puede ser interesante comentar cómo aplicar ciertas técnicas del resto de subdominios en este.

A continuación, como se ve en la figura 5.9, presentamos cada control como estaría ligado a las diferentes áreas de protección previamente presentadas.

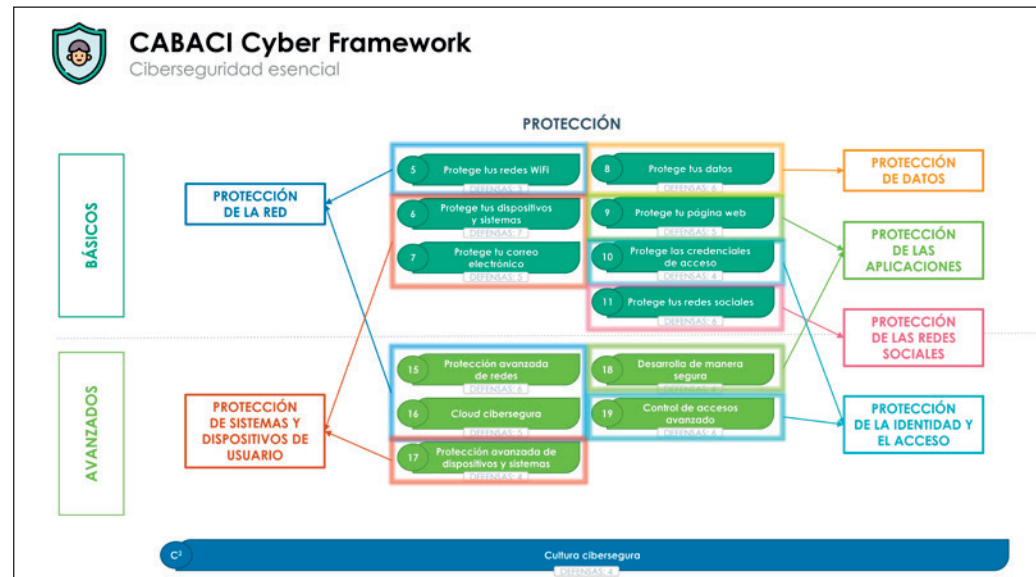


Figura 5.9. Framework CABACI. Protección. Subdominios.

Protección de la red

El concepto más sencillo de una red es un conjunto de dos ordenadores conectados mediante un cable compartiendo datos y recursos. Extendiendo el concepto más sencillo, tenemos las grandes redes de Internet, que nos permiten conectar dos puntos del planeta a través de una red de datos, independientemente de lo separados que estén geográficamente y de manera totalmente transparente para los usuarios. Pero la evolución de las redes y, sobre todo, la evolución del acceso a las redes ha originado la necesidad de aplicar medidas de seguridad. Un tipo de seguridad que a veces se olvida incorporar sobre la red de comunicaciones que soporta toda la red de datos, pero que es igual de vulnerable que un sistema o una aplicación. Podríamos hacer una gran introducción con todos los conceptos de infraestructuras de redes, desde comentar el modelo de capas OSI hasta explicar al detalle los protocolos TCP y UDP, pero consideramos que es más interesante, por el objetivo que tiene el libro y el capítulo, ir directamente a comentar la seguridad en la red desde un punto de vista más práctico, detallando las herramientas y arquitecturas que se pueden implementar para mitigar o reducir riesgos en este entorno.

Una infraestructura de red no ofrece directamente seguridad, es necesario disponer de una infraestructura de seguridad convergente con la red de datos. Además, la seguridad de la red no se basa en un método concreto, sino que utiliza un conjunto de barreras que defienden la infraestructura de diferentes formas. Incluso en el caso de que falle una solución, se mantendrán otras que protegerán a la infraestructura y a la información de una gran variedad de ataques a la red. La seguridad en la red permitirá:

- Proteger la infraestructura contra ataques, tanto internos como externos. Las amenazas se pueden originar tanto dentro como fuera de la estructura de una red.
- Garantizar la privacidad de todas las comunicaciones, en cualquier lugar y en cualquier momento. Los usuarios pueden acceder a la red desde casa o mientras se desplazan con la garantía de que sus comunicaciones serán privadas y estarán protegidas.
- Controlar el acceso a la información mediante la identificación y autenticación de los usuarios y sus sistemas.
- Transformar la red en una zona confiable.

Firewalls

Una *firewall* es un sistema o un conjunto de sistemas encargado de controlar las comunicaciones entre dos o más redes. Este se encarga de analizar, paquete a paquete, todo el tráfico que entra o sale de nuestra red, es decir, el *firewall* es la primera medida

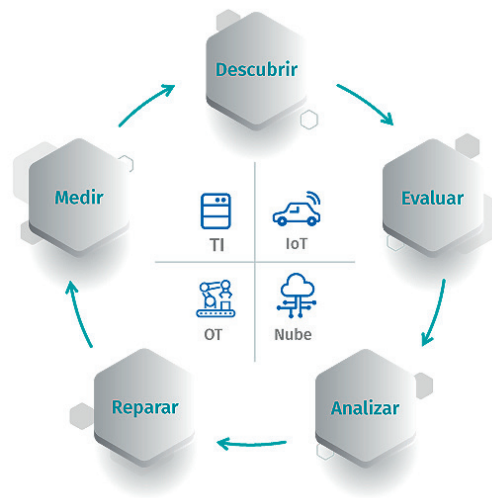


Figura 5.19. Ejemplo de proceso de gestión de vulnerabilidades. Fuente: Tenable (<https://es-la.tenable.com/blog/vulnerability-management-fundamentals-what-you-need-to-know>).

Gobierno y control

Todo este conjunto de capas de seguridad sobre los dispositivos y sistemas, siguiendo un modelo de seguridad en profundidad, requiere de un gobierno y de una gestión a un alto nivel. Nos referimos sobre todo a las políticas, procedimientos y tecnologías que una organización utiliza para supervisar y administrar sus dispositivos y servidores. La implementación efectiva de este dominio puede mejorar significativamente la postura de seguridad de una organización al proporcionar visibilidad sobre sus activos y permitir un control más granular sobre ellos.

Con respecto a la visibilidad y al inventariado de los mismos no vamos a entrar en mucho detalle, tradicionalmente es un área de IT el que gestiona todo ello, además en entornos pequeños o desarrollados completamente en nube es más fácil de realizar. Para lo demás, se puede contar con herramientas de tipo MDM y EPM.

Las soluciones MDM (*Mobile Device Management*) permiten a las organizaciones administrar, configurar y supervisar los dispositivos móviles utilizados por sus empleados. Esto puede incluir la aplicación de políticas de seguridad, la configuración de restricciones, la instalación o desinstalación de aplicaciones y la ejecución de acciones remotas, como el borrado de datos en caso de pérdida o robo del dispositivo.

Un ejemplo es Microsoft Intune, en la figura 5.20, la solución MDM de Microsoft basada en la nube. Administra el acceso de los usuarios y simplifica la administración de aplicaciones y dispositivos en muchos dispositivos, incluidos dispositivos móviles,

equipos de escritorio y puntos de conexión virtuales. Puede administrar usuarios y dispositivos, incluidos los dispositivos propiedad de la organización y los dispositivos de propiedad personal. Además, admite dispositivos Android, Android Open Source Project (AOSP), iOS/iPadOS, macOS y Windows.

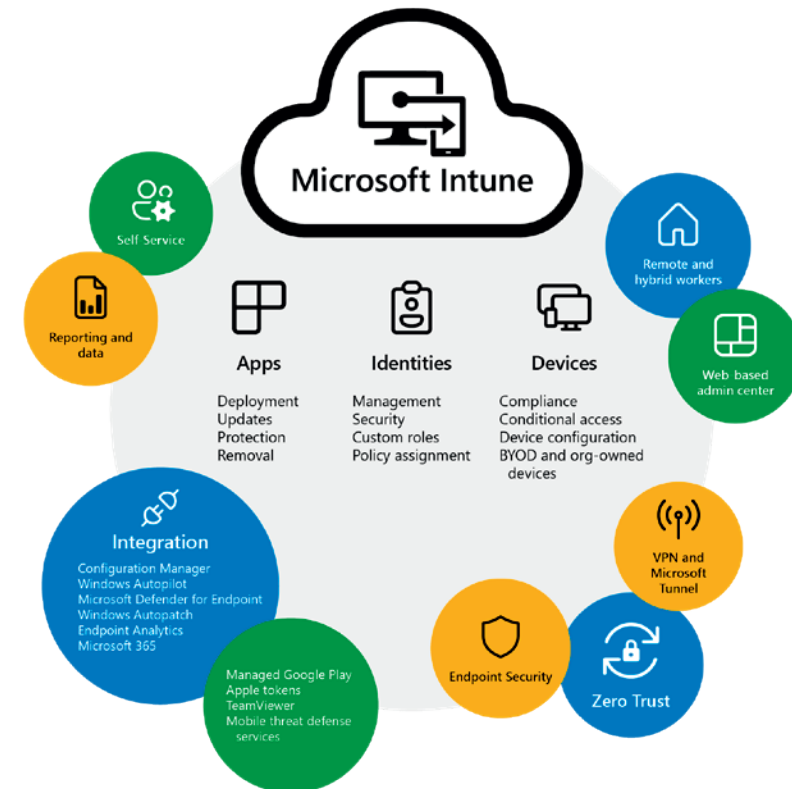


Figura 5.20. Características de Microsoft Intune. Fuente: Microsoft (<https://learn.microsoft.com/es-es/mem/intune/fundamentals/what-is-intune>).

Similar a las soluciones MDM, las soluciones EPM (*EndPoint Management*) proporcionan capacidades de administración y supervisión para servidores y estaciones de trabajo. Esto puede incluir la aplicación de configuraciones de seguridad, la supervisión del estado de los parches, la detección y respuesta a amenazas y la realización de análisis forenses.

Con respecto a la monitorización de los dispositivos y sistemas, se comentará en capítulos posteriores todo lo relacionado con la detección y respuesta, pero, como resumen, habría dos enfoques a tener en cuenta:

- **Visibilidad:** Los CASB proporcionan una visibilidad completa de la utilización de los servicios en la nube en una organización, permitiendo a los administradores de seguridad entender cómo se están usando estos servicios y por quién.
- **Cumplimiento:** Los CASB ayudan a las organizaciones a cumplir con las regulaciones de protección de datos y privacidad, proporcionando funciones como el cifrado de datos, la tokenización y las políticas de retención de datos.
- **Control de acceso:** Los CASB pueden aplicar políticas de control de acceso, asegurando que solo los usuarios autorizados puedan acceder a ciertos servicios o datos en la nube.
- **Protección de datos:** Los CASB pueden proporcionar funciones de protección de datos, como prevención de pérdida de datos (DLP), que pueden identificar y proteger los datos sensibles.
- **Protección contra amenazas:** Los CASB también pueden detectar y bloquear ciertas amenazas, como *malware* y ataques de ingeniería social.

Todas las herramientas donde hay un componente de análisis de la actividad del usuario permiten que se pueda considerar la puesta en marcha de alguna solución o enfoque de análisis de usuarios o, como se ha redefinido el concepto, una protección dinámica de usuarios (DUP, *Dynamic User Protection*). Estas soluciones se pueden integrar con el DLP y el CASB para tenerlas como fuentes de información y también para usar sus capacidades de respuesta para bloquear activamente las acciones que se consideren no autorizadas de forma dinámica, como se ve en la figura 5.27.

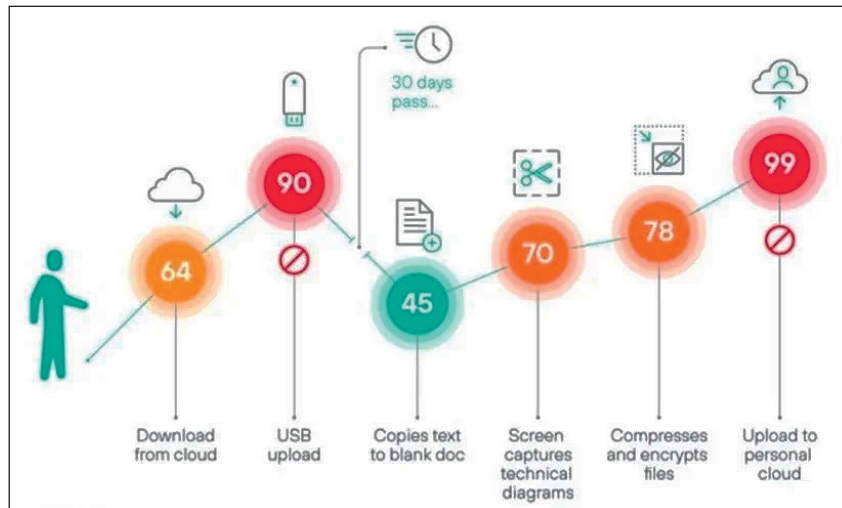


Figura 5.27. Acciones llevadas a cabo por un usuario y su nivel de riesgo asociado. Fuente: Forcepoint (<https://www.forcepoint.com/blog/insights/democratizing-uam>).

Los DUP consideran que cada usuario tiene un patrón de comportamiento único y normal dentro de una red o sistema. Cualquier actividad que se desvíe de este patrón normal podría ser indicativa de un comportamiento potencialmente malicioso o de un incidente de seguridad. Generalmente utilizan técnicas de aprendizaje automático y análisis de comportamiento para establecer un perfil de actividad normal para cada usuario. Esto puede incluir cosas como los sistemas a los que suelen acceder, los tipos de archivos con los que trabajan, los horarios en los que suelen estar activos, y más. Cada acción entonces comienza a ser "puntuada" con un *scoring* estableciendo así un perfil de riesgo donde actuar a partir de ciertos umbrales.

Privacidad

Desde el 25 de mayo de 2018 es de aplicación el Reglamento (UE) 2018/679 del Parlamento Europeo y del Consejo, en vigor desde el 27 de abril de 2018, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos y por el que se deroga la Directiva 95/46/CE. Aparece, por tanto, el GDPR (*General Data Protection Regulation*, Reglamento General de Protección de Datos), en la figura 5.28.

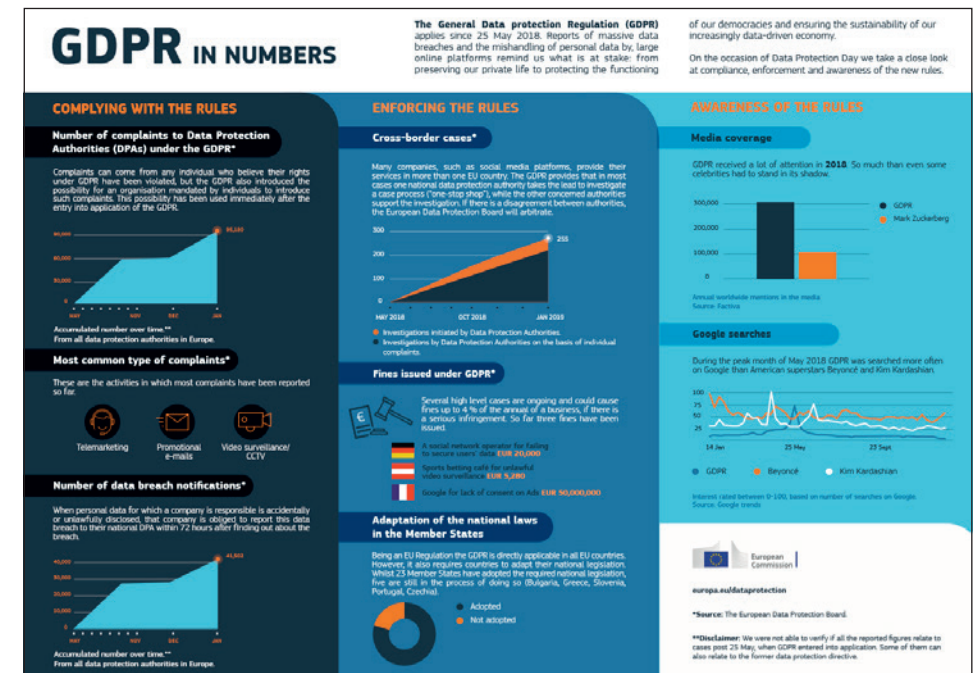


Figura 5.28. Infografía sobre la aplicación de GDPR. Fuente: <https://ec.europa.eu>.

Defensa 18.3. Auditoría de código y pruebas de intrusión

- **Tipo de control:** Avanzado.
- **Madurez de mi control:** ¿Se realizan auditorías de código y pruebas de intrusión de manera regular y sistemática en todas las aplicaciones de la compañía, y se implementan rápidamente las correcciones necesarias?
- **Medición de la madurez:**
 - **Nivel 1-En riesgo:** No se realizan auditorías de código ni pruebas de intrusión en las aplicaciones de la empresa.
 - **Nivel 2-Incompleto:** Se realizan auditorías de código o pruebas de intrusión de manera irregular o solamente en algunas aplicaciones.
 - **Nivel 3-Adaptativo:** Se realizan auditorías de código y pruebas de intrusión de manera regular y sistemática en todas las aplicaciones de la empresa, y se implementan rápidamente las correcciones necesarias.

Esta defensa se refiere a la realización regular de auditorías de código y pruebas de intrusión (*pentesting*) para identificar y solucionar vulnerabilidades en las aplicaciones. Las auditorías de código implican el análisis del código fuente de la aplicación para identificar fallos de seguridad, mientras que las pruebas de intrusión implican la simulación de ataques cibernéticos para evaluar la seguridad de la aplicación.

Algunos ejemplos de aplicación del control son:

- Utilización de herramientas de análisis de código estático (SAST) para revisar el código fuente en busca de problemas de seguridad.
- Contratación de un equipo de pruebas de intrusión para simular ataques cibernéticos y evaluar la resistencia de la aplicación.
- Implementación de un proceso para corregir rápidamente cualquier vulnerabilidad identificada durante las auditorías de código o las pruebas de intrusión.

Defensa 18.4. Gestión segura de las sesiones de usuario

- **Tipo de control:** Avanzado.
- **Madurez de mi control:** ¿Se gestionan de manera segura las sesiones de usuario en las aplicaciones, utilizando técnicas de seguridad y realizando auditorías regulares para asegurar su eficacia?

- **Medición de la madurez:**
 - **Nivel 1-En riesgo:** No se gestionan adecuadamente las sesiones de usuario o no se utilizan técnicas de seguridad en la gestión de las sesiones.
 - **Nivel 2-Incompleto:** Se utilizan algunas técnicas de seguridad para la gestión de las sesiones, pero no de manera completa o sistemática.
 - **Nivel 3-Adaptativo:** Se gestiona de forma segura las sesiones de usuario, utilizando técnicas de seguridad y realizando auditorías regulares para asegurar su eficacia.

Esta defensa implica el uso de prácticas de seguridad para gestionar las sesiones de usuario en las aplicaciones web. Esto incluye técnicas como el cierre automático de las sesiones después de un periodo de inactividad, la reautenticación antes de realizar acciones sensibles y el uso de *tokens* de sesión seguros y únicos.

Algunos ejemplos de aplicación del control son:

- Uso de *tokens* de sesión seguros y únicos para cada sesión y usuario.
- Configuración de un tiempo de espera de la sesión tras un periodo de inactividad del usuario.
- Requerimiento de reautenticación para las transacciones sensibles o cambios en la configuración del usuario.

Defensa 18.5. Verificación de dependencias y componentes de terceros

- **Tipo de control:** Avanzado.
- **Madurez de mi control:** ¿Existe un proceso para verificar la seguridad de las dependencias y los componentes de terceros utilizados en las aplicaciones de la compañía?
- **Medición de la madurez:**
 - **Nivel 1-En riesgo:** No existe un proceso formal para la verificación de dependencias y componentes de terceros.
 - **Nivel 2-Incompleto:** Existe un proceso para la verificación de dependencias y componentes de terceros, pero no se sigue de manera consistente o completa.
 - **Nivel 3-Adaptativo:** Existe un proceso bien definido y seguido para la verificación de dependencias y componentes de terceros, que incluye herramientas automáticas y evaluación de proveedores.

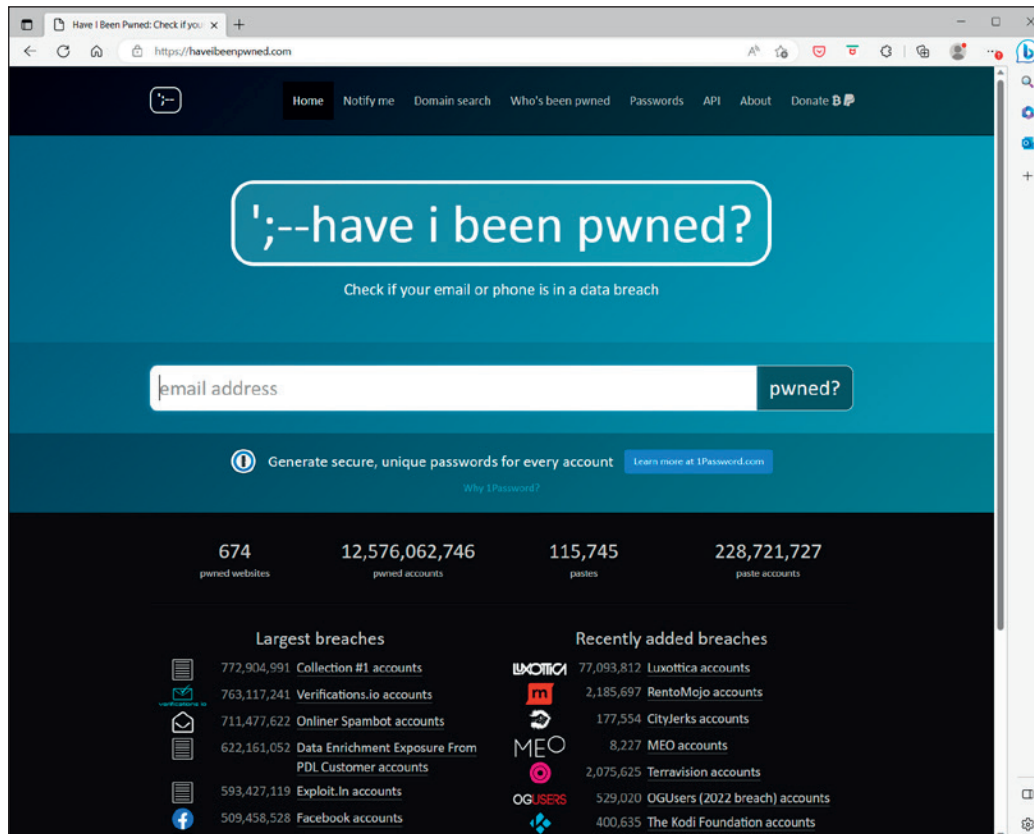


Figura 6.4. Have I Been Pwned.

Mantenerse informado sobre ataques de ciberseguridad

Las pequeñas empresas y emprendedores pueden mantenerse informados sobre las últimas tendencias en ciberseguridad y las amenazas actuales mediante la lectura de blogs de seguridad, boletines informativos y seguimiento de las noticias relacionadas con ciberseguridad. Esto les ayudará a tomar medidas preventivas y estar preparados para cualquier incidente.

Un posible vía para hacerlo es a través de **Google Alerts**. Esta herramienta permite a los usuarios recibir alertas de Google en tiempo real sobre cualquier término o frase que deseen monitorizar en la web. Por ejemplo, una empresa podría establecer alertas para su nombre de marca o información de contacto, lo que les permitiría recibir notificaciones si aparece información sospechosa o comprometida.

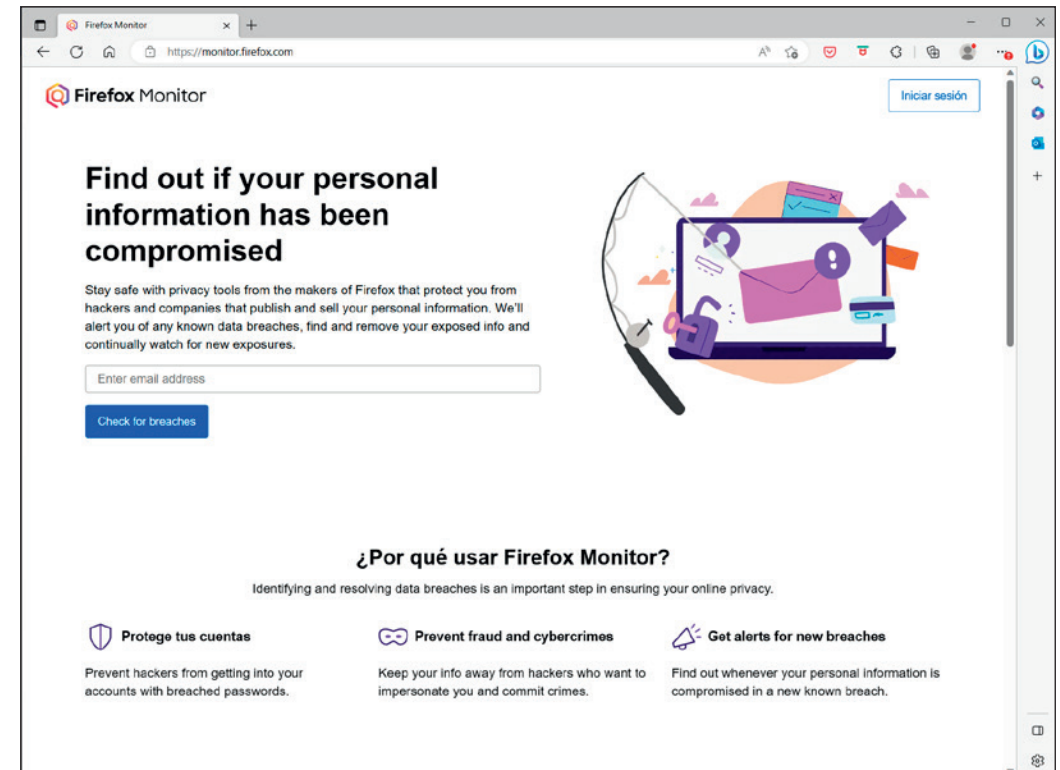


Figura 6.5. Firefox Monitor.

Para crear una alerta en Google, sigue estos pasos:

- Ve a la página de Google Alerts en tu navegador (<https://www.google.com/alerts>).
- En el cuadro de búsqueda, introduce la palabra clave o frase que deseas monitorizar. Puedes utilizar comillas para buscar una frase exacta.
- Selecciona el tipo de resultados que deseas recibir: Todo, Noticias, Blogs, Vídeos, Discusiones o Libros.
- Selecciona la frecuencia con la que deseas recibir alertas: Una vez al día o Tan pronto como se produzcan.
- Indica el correo electrónico donde deseas recibir las alertas.
- Haz clic en Crear alerta.

Para obtener más información sobre cómo configurar y utilizar Google Alerts, puedes consultar la guía oficial de Google en el siguiente enlace: <https://support.google.com/alerts/answer/4815696?hl=es>.

Defensas-Avanzadas

En el dominio de **Detección, respuesta y resiliencia** presentamos las defensas avanzadas. Una vez que hemos cubierto nuestras defensas básicas, es decir, que tenemos un plan para responder a un ataque, copias de seguridad y estamos al día con los últimos ataques, creemos que es momento de elevar el nivel de madurez de nuestras defensas, siempre y cuando nuestra empresa tenga suficiente envergadura para ello.

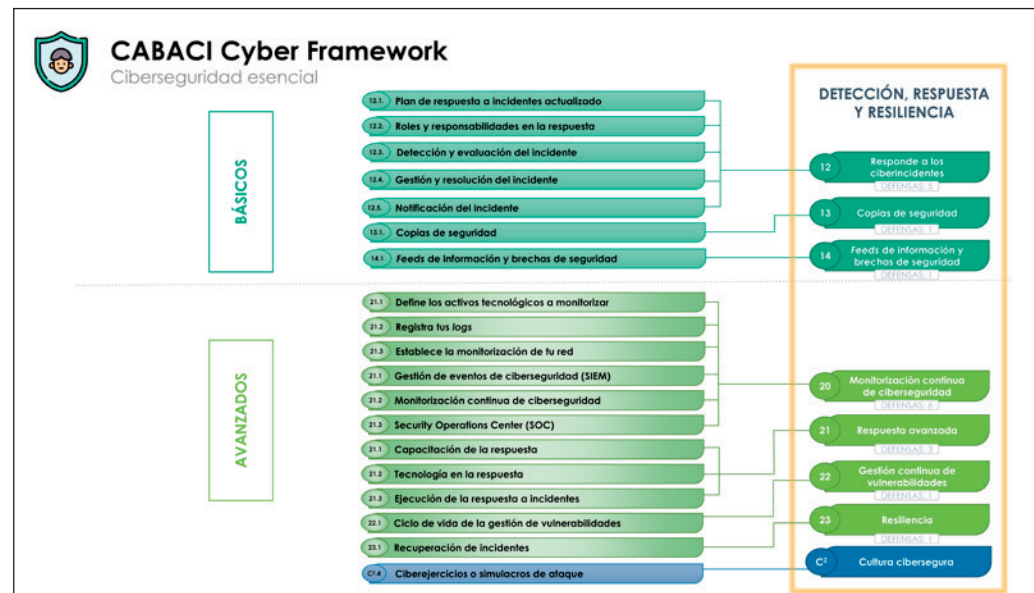


Figura 6.6. Framework CABACI-Detección respuesta y resiliencia detallado-Avanzados.

Disponer de buenas capacidades de detección es imprescindible para saber cuándo un ataque está ocurriendo. Nos permitirá actuar a tiempo para evitar que sea exitoso y, por lo tanto, se convierta en un incidente de seguridad.

El dominio se compone de los siguientes controles y defensas que iremos detallando uno por uno con ejemplos prácticos, para que se pueda comprender cómo desarrollar las defensas para su propio negocio.

- **Control 20. Monitorización continua de ciberseguridad:**
 - Defensa 20.1. Define los activos tecnológicos a monitorizar.
 - Defensa 20.2. Registra tus logs.
 - Defensa 20.3. Establece la monitorización de tu red.

- Defensa 20.4. Monitorización continua de ciberseguridad.
- Defensa 20.5. Gestión de eventos de ciberseguridad (SIEM).
- Defensa 20.6. Security Operations Center.
- **Control 21. Respuesta avanzada:**
 - Defensa 21.1. Capacitación de la respuesta.
 - Defensa 21.2. Tecnología en la respuesta.
 - Defensa 21.3. Ejecución de la respuesta a incidentes.
- **Control 22. Gestión continua de vulnerabilidades:**
 - Defensa 22.1. Ciclo de vida de la gestión de vulnerabilidades.
- **Control 23. Resiliencia:**
 - Control 23.1. Recuperación de incidentes.
- **Control C². Cultura cibersegura:**
 - Defensa C².1. Ciberejercicios o simulacros de ataque.
 - Defensa C².2. Plan de continuidad de negocio.

Control 20. Monitorización continua de ciberseguridad

La detección temprana de amenazas no es solo cuestión de prevenir los ataques, sino también de detectarlos lo antes posible. La monitorización continua permite identificar actividades sospechosas, lo que permite tomar medidas inmediatas para mitigar el impacto de un ataque o evitar daños mayores.

Defensa 20.1. Define los activos tecnológicos a monitorizar

- **Tipo de control:** Avanzado.
- **Madurez de mi control:** ¿Se han definido la prioridad de los activos tecnológicos a monitorizar?
- **Medición de la madurez:**
 - **Nivel 1-En riesgo:** No se han definido los activos tecnológicos prioritarios a monitorizar.
 - **Nivel 2-Incompleto:** Se han definido los activos tecnológicos prioritarios a monitorizar.
 - **Nivel 3-Adaptativo:** Se han definido los activos tecnológicos prioritarios a monitorizar y además existe un inventario de activos formal donde se informa de esto.

■ **Riesgo 3: Multas:**

- Madurez AS IS: 0,9.
- Madurez TO BE: 1,7.

Tabla 7.19. Macarena Bakes. Multas.

	MADUREZ 3	MADUREZ 2	MADUREZ 1
Datos comprometidos	Internos generales	Sensibles regulados con controles compensatorios o paliativos y un plan de mejora	Sensibles regulados sin controles compensatorios o paliativos
Impacto en negocio (multas)	Sin impacto	Cerca del 2 % de los ingresos anuales	Máximo el 4 % de los ingresos anuales

A continuación, presentamos algunas ideas más para que el lector lo pueda utilizar en sus ejercicios:

■ **Riesgo 4: Pérdida de clientes a otros competidores:**

- Madurez AS IS: 1,5.
- Madurez TO BE: 2,1.

Tabla 7.20. Macarena Bakes. Pérdida de clientes a otros competidores.

	MADUREZ 3	MADUREZ 2	MADUREZ 1
Pérdida de clientes	Alrededor del 5 %	Alrededor del 10 %	Alrededor del 20 %
Impacto en negocio	€	€€	€€€

■ **Riesgo 5: Daño reputacional:**

- Madurez AS IS: 1,8.
- Madurez TO BE: 2,3.

Tabla 7.21. Macarena Bakes. Daño reputacional.

	MADUREZ 3	MADUREZ 2	MADUREZ 1
Impacto en la marca o reputación de la empresa	Bajo	Medio	Alto
Impacto en negocio	€	€€	€€€

■ **Riesgo 6: Responsabilidad legal y penal para empleados y directivos:**

- Madurez AS IS: 1,2.
- Madurez TO BE: 1,8.

Tabla 7.22. Macarena Bakes. Responsabilidad legal y penal para empleados y directivos.

	MADUREZ 3	MADUREZ 2	MADUREZ 1
Responsabilidad	Responsabilidad fiduciaria, penal o legal	Responsabilidad fiduciaria, penal o legal Responsabilidad fiduciaria, penal o legal	Responsabilidad fiduciaria, penal o legal Responsabilidad fiduciaria, penal o legal
Multas	€	€€	€€€

■ **Riesgo 7. Pérdida del valor en las acciones:**

- Madurez AS IS: 1,1.
- Madurez TO BE: 1,5.

Tabla 7.23. Macarena Bakes. Pérdida del valor de las acciones.

	MADUREZ 3	MADUREZ 2	MADUREZ 1
Impacto en el valor	Bajo	Medio	Alto
Impacto en negocio	€	€€	€€€

Podemos incluso cuantificarlo más (por ejemplo, si el valor de una acción fuera 1 = 290 euros), tendríamos 1 = 230; 1 = 78; 1 = 24.

■ **Riesgo 8: Interrupción de un servicio esencial, crítico:**

- Madurez AS IS: 1,17.
- Madurez TO BE: 2,3.

Tabla 7.24. Macarena Bakes. Interrupción de un servicio esencial.

	MADUREZ 3	MADUREZ 2	MADUREZ 1
Duración de la disrupción	Minutos	Horas	Días
Impacto en negocio	€	€€	€€€
Impacto en salud y bienestar (si aplica)	Bajo	Medio	Alto

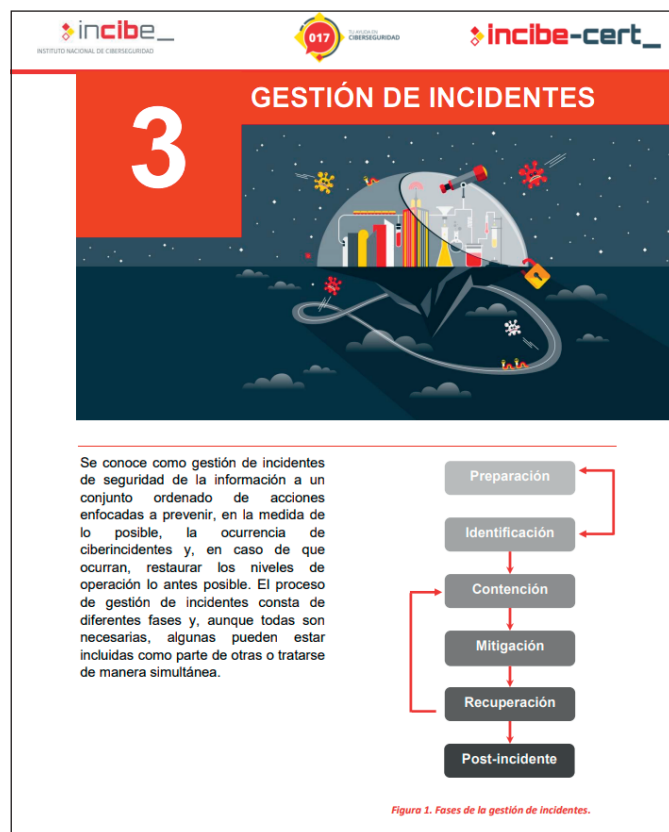


Figura 9.8. Fases de la gestión de incidentes según INCIBE.

Fuente: Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía (https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_gestion_ciberincidentes_sector_privado.pdf).

INCIBE-CERT, tal y como detalla en su página web, como centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España, tiene dentro de sus funciones de respuesta ante incidentes las siguientes:

- Ofrecer soporte técnico y proporcionar información para ayudar en la resolución de los incidentes de ciberseguridad dentro su ámbito de actuación.
- Emplear técnicas de detección temprana de incidentes, notificando a los afectados, para que puedan tomar medidas.
- Mantener el contacto con los proveedores de Internet y otros CERT (nacionales e internacionales), notificando el incidente, a fin de que se puedan tomar medidas que limiten o impidan su continuidad.

Concienciación

La concienciación en ciberseguridad es una parte fundamental de cualquier estrategia de seguridad. Para los emprendedores, este aspecto puede ser aún más crítico. Por lo general, los emprendedores manejan recursos limitados y, a menudo, son el objetivo de los ciberataques. Por lo tanto, cada individuo en su organización tiene un papel vital que desempeñar para mantener la seguridad de la información y los sistemas.

Lo primero es adquirir un conocimiento básico sobre ciberseguridad. Los emprendedores deben entender qué es, cuáles son los riesgos y amenazas más comunes y cómo pueden impactar en su negocio. Esta educación debe ser continua, dado que la ciberseguridad es un campo en constante cambio, con nuevas amenazas y vulnerabilidades surgiendo constantemente. Por lo tanto, es esencial mantenerse al día sobre las últimas tendencias y amenazas de ciberseguridad.

Afortunadamente, existen numerosos recursos educativos gratuitos en línea que pueden ayudar a los emprendedores a mejorar sus habilidades y conocimientos en ciberseguridad. Estos cursos cubren una amplia gama de temas, desde fundamentos de ciberseguridad hasta la protección contra amenazas específicas y la gestión de incidentes de seguridad. Algunos de estos cursos incluso ofrecen certificaciones, lo que puede aumentar la credibilidad de un emprendedor en su campo y demostrar su compromiso con la seguridad de la información. Los beneficios de los cursos de ciberseguridad en línea son varios. En primer lugar, son accesibles desde cualquier lugar y en cualquier momento, lo que significa que los emprendedores pueden aprender a su propio ritmo y según su propio horario. Además, ofrecen contenido actualizado y relevante, impartido por expertos en la materia. Algunos de estos cursos también proporcionan ejercicios prácticos y simulaciones, lo que permite a los emprendedores aplicar lo que han aprendido a escenarios de la vida real.

Las buenas prácticas de ciberseguridad deben aplicarse en todas las actividades diarias. Esto puede incluir aspectos tan sencillos como el uso de contraseñas seguras, la protección de la información sensible y la aplicación de las actualizaciones y parches de seguridad en el momento adecuado.

En caso de tener empleados, es vital que también estén formados en ciberseguridad. Necesitan entender las amenazas comunes y cómo su acción puede ayudar a prevenir los ciberataques. Por lo tanto, es crucial establecer una cultura de ciberseguridad en la organización, en la que la seguridad sea una prioridad en todos los niveles.

Finalmente, es importante estar preparado para los incidentes. Los emprendedores deben saber qué hacer en caso de un ciberincidente, lo que incluye tener un plan de respuesta a incidentes y practicar regularmente escenarios de incidentes de seguridad. En última instancia, los emprendedores tienen una responsabilidad única de proteger sus negocios de los ciberataques, y una fuerte conciencia en ciberseguridad puede ser su mejor defensa.

¿Sabías que el 60 % de las empresas que son atacadas cierra su negocio a los 6 meses? En la nueva era digital es vital elaborar una adecuada estrategia de ciberseguridad que nos permita protegernos de las amenazas de ciberseguridad y de los nuevos actores de amenazas del ciberespacio. El cibercrimen tiene un coste de trillones de euros superando al PIB de muchos países.

¿Soy un objetivo de los ciberdelincuentes? ¿Cuáles son las amenazas de mi negocio? ¿Quiénes son los actores de amenazas? ¿Qué motivaciones tienen? ¿Tengo una adecuada estrategia de ciberseguridad que me ayude a evitar ataques actuales como fuga de información, *ransomware* o ataques a terceros?

Este es un libro práctico que muestra la manera de elaborar tu estrategia de ciberseguridad paso a paso. En el libro elaboramos el nuevo y sencillo marco de ciberseguridad CABACI que te permitirá evaluar tu nivel de madurez en ciberseguridad. Especialmente útil para pymes, autónomos o *influencers*, personas que se quieran introducir en la ciberseguridad de manera fácil, tanto técnicas como de negocio, CEO, XEO, responsables de ciberseguridad, CISOS y cualquier otra persona que necesite guiarse al construir su estrategia de ciberseguridad.

Hablamos de la importancia de entender tu negocio y tecnología, de identificar a tus *stakeholders* y que estén comprometidos con tu programa de ciberseguridad que aprenderás a construir, de cómo proteger tu negocio frente a las amenazas y de cómo detectar, responder y recuperarte de un incidente de ciberseguridad, así como comunicarlo adecuadamente. En definitiva, una guía práctica que detalla paso a paso cómo construir una estrategia de ciberseguridad adaptada a ti. ¿Preparado?



www.anayamultimedia.es

