

MAPA GLOBAL DE CIBERATAQUES: CAUSAS Y MITIGACIÓN

Top 10 ataques más comunes:

1. **Phishing / Spear-phishing**
 1. Por qué: Es barato, escalable y explota el eslabón humano (usuarios distraídos).
 2. Mitigación: Formación continua + simulacros; filtros de correo (SPF/DKIM/DMARC); MFA universal; detección de URLs y anexos maliciosos.
2. **Ataques contra credenciales (Credential stuffing / Brute force / Password spraying)**
 1. Por qué: Muchas personas reutilizan contraseñas y las brechas públicas alimentan ataques automatizados.
 2. Mitigación: MFA (preferiblemente FIDO/Hardware), rate-limiting, bloqueo/alertas por patrones, breach monitoring y políticas de contraseña fuertes.
3. **Ransomware**
 1. Por qué: Alto ROI para atacantes; automatizable y rentable (extorsión).
 2. Mitigación: Backups offsite y verificados; segmentación de red; EDR con detección de comportamiento; least privilege y aplicar parches rápido.
4. **Inyección SQL (SQLi)**
 1. Por qué: Muchas aplicaciones aún usan entradas sin sanear y bases de datos accesibles.
 2. Mitigación: Prepared statements / ORM, validación de entrada, least privilege en BD, WAF y pentesting regular.
5. **Cross-Site Scripting (XSS)**
 1. Por qué: Sitios dinámicos y campos de usuario mal escapados siguen presentes en multitud de aplicaciones web.
 2. Mitigación: Escape/encode de salida, CSP, HttpOnly/SameSite cookies, revisión de plantillas y sanitización de inputs.
6. **Malware general (Trojans / Botnets / C2 / Fileless)**
 1. Por qué: Vectores múltiples (correo, web, USB, descargas) y gran disponibilidad de toolkits.
 2. Mitigación: EDR/antivirus, control de ejecución (AppLocker, policies), segmentación, detección de beaconing y hardening de endpoints.
7. **Cloud misconfiguration / Exposición de datos (S3 buckets, storage público)**
 1. Por qué: Rapidez de despliegue y falta de control sobre IaC o permisos llevan a exposiciones accidentales.
 2. Mitigación: IaC scanning, CSPM, least privilege, auditorías periódicas, logging y alertas sobre buckets públicos.
8. **Denegación de Servicio (DoS / DDoS)**
 1. Por qué: Fácil de lanzar con botnets; impacta disponibilidad y es usado como distracción.
 2. Mitigación: CDN / scrubbing services (Cloudflare, proveedores cloud), rate limiting, diseño elástico y reglas en perimeter.
9. **Server-Side Request Forgery (SSRF) / Remote Code Execution (RCE) relacionadas a servicios**
 1. Por qué: APIs y servicios que permiten al servidor hacer peticiones externas son vectores ricos para atacar metadatos o recursos internos.
 2. Mitigación: Whitelists de destinos, validación de URLs, bloqueo de accesos a metadata (IMDS), WAF y least privilege en roles.
10. **Supply-chain / Dependencias comprometidas (repos, imágenes, librerías)**
 1. Por qué: Muchas organizaciones dependen de terceros — un proveedor o imagen comprometida impacta a muchos.
 2. Mitigación: SCA (Software Composition Analysis), firmar imágenes/artifacts, escaneo de CI/CD, políticas de revisión y gestión de proveedores.



TODOS LOS TIPOS DE ATAQUES

Ataques de red y transporte

- **Denegación de servicio (DoS) / Distribuido (DDoS)**
 - *Qué es (concepto):* Abrumar un recurso (ancho de banda, CPU, conexiones) hasta que deje de servir.
 - *Mitigación:* Filtrado en perímetro, WAF/DoS mitigation (Cloudflare, AWS Shield), rate-limiting, escalado/elástica, CDN, blackholing y scrubbing. Monitoreo de tráfico e IPS/flow analysis.
- **MITM — Man-in-the-Middle (ARP spoofing, DNS spoofing, TCP hijacking)**
 - *Qué es:* Interceptar/alterar comunicaciones entre dos partes.
 - *Mitigación:* HTTPS/TLS con verificación correcta, HSTS, DNSSEC, autenticación mutua, segmentación de red, uso de switches vs hubs, detección ARP anomalies.
- **Sniffing / packet capture**
 - *Qué es:* Capturar tráfico en la red para obtener credenciales u otra información.
 - *Mitigación:* Cifrado en tránsito (TLS, VPN), 802.1X, evitar texto plano (no usar HTTP, Telnet, FTP sin cifrado).
- **ARP poisoning / spoofing**
 - *Qué es:* Manipular tablas ARP para redirigir tráfico.
 - *Mitigación:* Static ARP en hosts críticos, switch port security, DAI (Dynamic ARP Inspection), IDS/IPS.
- **IP spoofing / session hijacking**
 - *Qué es:* Forjar direcciones IP o secuestrar sesiones activas.
 - *Mitigación:* Ingress/Egress filtering, tokens de sesión seguros, TLS, control de sesiones.
- **Ataques DNS (cache poisoning, amplification)**
 - *Qué es:* Envenenar cache DNS o usar DNS para amplificación DDoS.
 - *Mitigación:* DNSSEC, rate-limiting, usar resolvers seguros, monitoreo de patrones DNS.

2) Ataques a aplicaciones web

- **Inyección SQL (SQLi)**
 - *Qué es:* Insertar código SQL malicioso en entradas para manipular BD.
 - *Mitigación:* Consultas parametrizadas (prepared statements), ORM seguro, validación y saneamiento de inputs, WAF, least privilege en BD, pruebas de pentest.
- **Cross-Site Scripting (XSS) — reflejado, almacenado, DOM**
 - *Qué es:* Inyectar scripts en páginas que se ejecutan en el navegador de la víctima.
 - *Mitigación:* Escape/encode de salida, Content Security Policy (CSP), validación de entrada, HttpOnly en cookies.
- **Cross-Site Request Forgery (CSRF)**
 - *Qué es:* Forzar a un usuario autenticado a ejecutar acciones no deseadas.
 - *Mitigación:* Tokens anti-CSRF, SameSite cookies, doble submit cookies, validación de origen.
- **Remote Code Execution (RCE)**
 - *Qué es:* Ejecutar código arbitrario en el servidor a través de vulnerabilidades.
 - *Mitigación:* Parches, limitación de privilegios, WAF, ejecución en entornos aislados (contenerización), validación estricta de inputs.
- **Local / Remote File Inclusion (LFI / RFI)**



- o *Qué es:* Incluir archivos locales o remotos en ejecución del servidor.
 - o *Mitigación:* Validación de rutas, uso de path canonicalization, no permitir include dinámico basado en input, políticas de permisos.
- **File upload vulnerabilities**
 - o *Qué es:* Subida de archivos maliciosos (web shells, scripts).
 - o *Mitigación:* Validación de tipos/MIME, renombrado, escaneo antivirus, sandbox para procesamiento, restricciones de ejecución.
- **Server-Side Request Forgery (SSRF)**
 - o *Qué es:* Hacer que el servidor haga peticiones a recursos internos/externos controlados por el atacante.
 - o *Mitigación:* Validar URLs, bloquear acceso a metadatos internas, listas blancas, timeout y rate-limits.
- **Broken authentication / session management**
 - o *Qué es:* Fallos en manejo de sesiones (tokens predecibles, expiración inapropiada).
 - o *Mitigación:* Tokens seguros, expiración, rotación, revocación, MFA, login throttling.
- **Business Logic Flaws**
 - o *Qué es:* Abusar de la lógica de negocio (ej. compra con saldo negativo).
 - o *Mitigación:* Revisiones de diseño, testeo funcional, validación de reglas en servidor.

3) Ataques de autenticación y credenciales

- **Brute force / password guessing**
 - o *Qué es:* Probar múltiples contraseñas hasta acertar.
 - o *Mitigación:* Rate-limiting, account lockout, MFA, detection de patterns.
- **Credential stuffing**
 - o *Qué es:* Reutilizar credenciales filtradas en otros servicios.
 - o *Mitigación:* MFA, detección de login anomalies, password policies y breach monitoring.
- **Password spraying**
 - o *Qué es:* Probar una lista pequeña de contraseñas comunes contra muchos usuarios.
 - o *Mitigación:* Same as brute force + monitoring, MFA.
- **Pass-the-Hash / Pass-the-Ticket**
 - o *Qué es:* Reutilizar hashes/tickets de autenticación para moverse lateralmente.
 - o *Mitigación:* Windows hardening (LSA protection), Kerberos protections, credential isolation, endpoint hardening, EDR.
- **MFA bypass (SIM swapping, OTP interception)**
 - o *Qué es:* Robar/evadir segundo factor.
 - o *Mitigación:* Uso de FIDO2/keys físicas, notificaciones de cambio, no usar SMS como primer factor.

4) Malware y software malicioso

- **Virus / Worms / Trojans**
 - o *Qué es:* Programas que dañan, replican o se disfrazan.
 - o *Mitigación:* EDR/antivirus, segmentación, políticas de ejecución, actualizaciones.
- **Ransomware**
 - o *Qué es:* Cifrar datos y pedir rescate.
 - o *Mitigación:* Backups offsite y probados, segmentación, EDR, least privilege, detección temprana (indicators de cifrado).
- **Spyware / Keyloggers**
 - o *Qué es:* Espiar usuario y robar credenciales.
 - o *Mitigación:* EDR, control de dispositivos, políticas de software.
- **Rootkits**



- o *Qué es:* Persistencia a nivel kernel/firmware ocultando presencia.
 - o *Mitigación:* Secure boot, monitorización de integridad, parches firmware, reimagenación.
- **Botnets / C2 (Command & Control)**
 - o *Qué es:* Red de dispositivos comprometidos controlados por atacante.
 - o *Mitigación:* Detección de beaconing, tráfico anómalo, sinkholing DNS, bloqueo de endpoints.
- **Fileless malware**
 - o *Qué es:* Ejecuta en memoria usando herramientas legítimas (PowerShell, WMI).
 - o *Mitigación:* Monitoring de comportamiento, restricciones de ejecución, EDR con detección de comportamiento.

5) Ingeniería social y ataques humanos

- **Phishing / spear-phishing**
 - o *Qué es:* Engaños para revelar credenciales o ejecutar acciones.
 - o *Mitigación:* Formación, simulacros, filtros de correo, DMARC/DKIM/SPF, MFA.
- **Vishing / smishing (voz / SMS)**
 - o *Qué es:* Engaños por teléfono o SMS.
 - o *Mitigación:* Formación, procesos de verificación, no usar SMS para MFA crítico.
- **Pretexting / baiting / quid pro quo**
 - o *Qué es:* Fingir autoridad o beneficios para obtener información.
 - o *Mitigación:* Procedimientos de verificación, cultura de seguridad.
- **Insider threats (maliciosos o negligentes)**
 - o *Qué es:* Empleados que filtran o dañan datos.
 - o *Mitigación:* DLP, least privilege, separación de funciones, monitoreo, políticas HR.

6) Criptografía y ataques relacionados

- **Cracking de hashes / rainbow tables**
 - o *Qué es:* Recuperar contraseñas a partir de hashes.
 - o *Mitigación:* Salting, KDFs (bcrypt, Argon2), políticas de contraseña.
- **Padding oracle / CBC attacks**
 - o *Qué es:* Explotar errores de padding en cifrados.
 - o *Mitigación:* Uso de modos autenticados (GCM), manejo correcto de errores.
- **Downgrade attacks (protocolo)**
 - o *Qué es:* Forzar uso de versiones inseguras (TLS 1.0).
 - o *Mitigación:* Configurar sólo versiones seguras, HSTS, evitar suites débiles.
- **Side-channel attacks (timing, power, electromagnetic)**
 - o *Qué es:* Extraer claves por señales físicas o temporales.
 - o *Mitigación:* Hardening hardware, constant-time implementations, shielding.

7) Wireless y Bluetooth

- **Evil Twin / Rogue AP**
 - o *Qué es:* AP falso para interceptar tráfico.
 - o *Mitigación:* WPA2/3 con EAP, 802.1X, certificados, VPN, detectar APS sospechosas.
- **KRACK / ataques a WPA/WPA2**
 - o *Qué es:* Vulnerabilidades en handshake Wi-Fi.
 - o *Mitigación:* Parches, usar WPA3, actualizaciones.
- **WEP cracking / weak crypto**



- o *Qué es:* Protocolos débiles fáciles de romper.
- o *Mitigación:* No usar WEP, migrar a WPA3, políticas de seguridad.

8) Cloud / servicios gestionados

- **Cloud misconfiguration (S3 buckets, Storage mispermits)**
 - o *Qué es:* Recursos expuestos por configuración.
 - o *Mitigación:* IaC scanning, CSPM tools, least privilege, auditorías, logging.
- **IAM abuse / privilege escalation**
 - o *Qué es:* Abuso de permisos en entorno cloud.
 - o *Mitigación:* Principle of least privilege, roles temporales, monitoring de actividades, MFA for console.
- **Server-Side Request Forgery (SSRF) en entornos cloud**
 - o *Qué es:* Atacar metadatos (p. ej. IMDS) para robar credentials.
 - o *Mitigación:* Bloquear accesos de instancias a metadatos, políticas de red, firewall de salida.
- **Supply-chain attacks en SaaS / containers**
 - o *Qué es:* Compromiso de dependencias o imágenes base.
 - o *Mitigación:* Scanning de imágenes, firmar artefactos, SCA (Software Composition Analysis).

9) Contenedores y virtualización

- **Container escape / VM escape**
 - o *Qué es:* Escapar del contenedor/VM al host.
 - o *Mitigación:* Namespace separation, seccomp, AppArmor/SELinux, actualizaciones, imágenes minimizadas.
- **Insecure container images / registry compromise**
 - o *Qué es:* Imágenes con malware o vulnerabilidades.
 - o *Mitigación:* Scan de imágenes, firmar imágenes, repos privados y audited.

10) API y servicios web modernos

- **API abuse (broken object-level auth, mass assignment)**
 - o *Qué es:* Abusar de endpoints REST/GraphQL para exfiltrar o manipular datos.
 - o *Mitigación:* Authn/Authz robusta, rate limiting, input validation, API gateway, logging.
- **Rate limit bypass / resource exhaustion via APIs**
 - o *Qué es:* Forzar consumo excesivo de recursos.
 - o *Mitigación:* Rate limits, quotas, circuit breaker patterns.

11) IoT y embebidos

- **Device compromise (default creds, firmware bugs)**
 - o *Qué es:* Dispositivos inseguros comprometidos.
 - o *Mitigación:* Cambiar credenciales por defecto, firmwares firmados, network segmentation, monitorización de IoT.
- **Botnet IoT (Mirai-like)**
 - o *Qué es:* Uso masivo de IoT para DDoS.
 - o *Mitigación:* Same as above + ISP cooperation, detection of C2 patterns.

12) Supply chain y third-party risk

- **Tercerización comprometida (dependencias, librerías, proveedores)**



- o *Qué es:* Vectores a través de terceros.
- o *Mitigación:* Vendor risk management, SCA, revisión de dependencias, políticas contractuales, monitorización de CVEs.

13) Data exfiltration y privacidad

- **Exfiltration over DNS / covert channels**
 - o *Qué es:* Sacar datos por canales discretos.
 - o *Mitigación:* DLP, monitorización DNS, egress filtering, anomaly detection.
- **Re-identification / deanonymization**
 - o *Qué es:* Cruzar datasets para identificar individuos.
 - o *Mitigación:* Minimización de datos, anonimización robusta, políticas de retención.

14) Advanced Persistent Threats (APT) y ataques dirigidos

- **APTs (multi-stage, persistencia, lateral movement)**
 - o *Qué es:* Ataques prolongados, dirigidos y sofisticados.
 - o *Mitigación:* EDR, threat hunting, segmentation, blue team maturity, threat intel, red/blue exercises.

15) Ataques físicos y hardware

- **Tampering / hardware implants / USB drops**
 - o *Qué es:* Inserción física de malware o manipulación.
 - o *Mitigación:* Control de acceso físico, policies USB, bloqueo de puertos, CCTV, inventario.
- **Side-channel físico (power analysis, EM)**
 - o *Qué es:* Extraer información de señales físicas.
 - o *Mitigación:* Shielding, diseño seguro hardware, constant-time crypto.

16) Técnicas de post-explotación (movimiento lateral, persistencia)

- **Credential harvesting, lateral movement, persistence**
 - o *Qué es:* Aprovechar acceso inicial para escalar y mantenerse.
 - o *Mitigación:* Least privilege, segmentation, EDR con detección de comportamiento, honeypots, logging centralizado.

17) Ataques a cadenas CI/CD y desarrollo

- **Compromiso de pipelines, secrets leakage en repos**
 - o *Qué es:* Robo de credenciales/keys en pipelines o repos públicos.
 - o *Mitigación:* Secrets manager, scanning de commits, inline secret detection, least privilege para deploy keys.

18) Ataques emergentes / especializados

- **Cryptojacking**
 - o *Qué es:* Uso no autorizado de recursos para minar criptomonedas.
 - o *Mitigación:* Monitor CPU usage, EDR, bloqueos en navegadores, patches.
- **Machine learning attacks (poisoning, model inversion)**
 - o *Qué es:* Manipular datos de entrenamiento o extraer información del modelo.
 - o *Mitigación:* Data validation, model hardening, differential privacy.

