CiberSeguridad 2026

1-¿Qué es la Ciberseguridad?

> **Definición:** La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales que tienen como objetivo acceder, cambiar o destruir información sensible.

Objetivo de ciberseguridad	Descripción breve
Protección de datos y sistemas informáticos	Salvaguardar la información y los recursos tecnológicos frente a ataques o daños.
Prevención de accesos no autorizados	Evitar que personas o programas no autorizados entren en sistemas o redes.
Garantía de confidencialidad e integridad	Asegurar que los datos se mantengan privados y sin alteraciones indebidas.
Continuidad del negocio digital	Mantener las operaciones y servicios activos incluso ante incidentes de ciberseguridad.

2-Principios

> Pilares fundamentales de la seguridad de la información

```
(Confidencialidad-Integridad-Disponibilidad)
```

Pilar CIA Triada	Definición
Confidencialidad	Solo usuarios autorizados ven la información
Integridad	Los datos no se alteran sin permiso
Disponibilidad	La información está accesible cuando se necesita

Confidencialidad

> Garantizar que la información solo es accesible para quienes tienen autorización

Amenaza	Ejemplos	Controles de seguridad
Ataques Man-in-the-Middle (MITM)	Interceptación de comunicaciones, manipulación de tráfico	Cifrado (TLS/SSL), validación de certificados

Amenaza	Ejemplos	Controles de seguridad
Robo de credenciales	Phishing, keyloggers, dumps de bases de datos	Autenticación multifactor (MFA), gestión segura de contraseñas
Acceso no autorizado	Escalada de privilegios, explotación de vulnerabilidades	Control de acceso (RBAC, IAM), parches de seguridad
Fuga de datos	Exfiltración de información sensible	Cifrado (AES, RSA), monitoreo y detección de anomalías

Integridad

> Asegurar que los datos son exactos, completos y no han sido alterados de forma no autorizada

Amenaza	Ejemplos	Controles de seguridad
Modificación de datos	Inyecciones SQL, XSS	Hashing (SHA-256, checksums), validación de entradas
Alteración de logs	Ocultar rastros de ataques	Firmas digitales, registros inmutables
Malware	Troyanos que modifican archivos del sistema	Sistemas de detección de intrusiones (IDS), análisis antivirus
Manipulación de configuraciones	Backdoors, mecanismos de persistencia	Firmas digitales, control de integridad y auditorías

Disponibilidad

> Garantizar que sistemas y datos estén accesibles cuando usuarios autorizados los necesiten

Amenaza	Ejemplos	Controles de seguridad
DDoS (Distributed Denial of Service)	Saturación de recursos, interrupción del servicio	Redundancia y alta disponibilidad (HA), mitigación de tráfico
Ransomware	Cifrado de datos y rescate económico	Backups automáticos (regla 3-2-1), planes de recuperación (DRP)
Sabotaje	Destrucción física o lógica de infraestructura	Planes de continuidad (BCP), controles físicos y lógicos
Fallos de hardware	Sin redundancia ni copias de seguridad	Redundancia (RAID, HA), backups automáticos, monitoreo proactivo

Principios Adicionales`

> Sumados a los CIA. Para garantizar la protección de la información

Principio de seguridad	Descripción breve
Autenticación	Verificar la identidad del usuario mediante credenciales o métodos biométricos.
Autorización	Definir permisos y privilegios de acceso según roles y necesidades.
No repudio	Garantizar que una acción no pueda ser negada por quien la realizó.
Trazabilidad	Registrar todas las acciones para auditorías y análisis forense.
Privacidad	Proteger datos personales contra accesos no autorizados o filtraciones.

`3-Conceptos Clave`

Fórmula: Riesgo = Amenaza × Vulnerabilidad × Impacto

3.1-Diccionario

Concepto	Definición	Ejemplo
Amenaza (Threat)	Potencial causa de daño que puede afectar un sistema o activo.	Hacker, malware, desastre natural
Vulnerabilidad (Vulnerability)	Debilidad o fallo que puede ser explotado por una amenaza.	Bug de software, mala configuración
Riesgo (Risk)	Probabilidad de que una amenaza aproveche una vulnerabilidad y cause impacto.	Probabilidad de ataque exitoso debido a una brecha
Exploit	Código o técnica que aprovecha una vulnerabilidad específica.	Script que explota una falla en una aplicación web
Payload	Código malicioso que se ejecuta tras la explotación de una vulnerabilidad.	Ransomware, shell reversa, troyano
Vector de ataque	Método o camino utilizado para comprometer un sistema o acceder a recursos sensibles.	Email, USB infectado, web maliciosa, red interna
Superficie de ataque	Conjunto total de puntos por donde un atacante puede intentar acceder o comprometer un sistema.	Puertos abiertos, APIs públicas, cuentas de usuario

Concepto	Definición	Ejemplo
Zero-day	Vulnerabilidad desconocida por el fabricante y sin parche disponible al momento del ataque.	Falla en software explotada antes de su divulgación
APT (Advanced Persistent Threat)	Ataque sofisticado, prolongado y dirigido, realizado por actores con recursos avanzados.	Grupo estatal infiltrando infraestructura crítica
IOC (Indicator of Compromise)	Evidencia o señal de que un sistema ha sido comprometido.	IP sospechosa, archivo modificado, hash de malware detectado
Hardening	Proceso de asegurar un sistema reduciendo su superficie de ataque.	Deshabilitar servicios innecesarios, aplicar parches
Sandboxing	Aislar aplicaciones o archivos en entornos controlados para analizar su comportamiento.	Ejecutar malware en entorno virtual para observación
Honeypot	Sistema trampa diseñado para atraer atacantes y estudiar sus técnicas.	Servidor falso que recopila información sobre ataques
Lateral movement	Acción de un atacante que, tras comprometer un punto, se desplaza internamente por la red.	Uso de credenciales robadas para acceder a otros equipos
Privilege escalation	Técnica mediante la cual un atacante obtiene permisos superiores a los inicialmente comprometidos.	Pasar de usuario limitado a administrador/root

3.2-Actores de Amenazas

Categoría	Tipo de atacante	Motivación o características	Ejemplo
Por motivación	**Cibercriminales**	Buscan beneficio económico mediante delitos digitales.	Ransomware, fraude financiero
	Hacktivistas	Actúan por motivos ideológicos, políticos o sociales.	Ataques DDoS por protestas
	Estados-nación	Realizan espionaje o sabotaje en interés geopolítico.	Ciberataques a infraestructuras críticas
	Insiders	Empleados o contratistas que abusan de su acceso interno.	Robo o filtración de información interna

Categoría	Tipo de atacante	Motivación o características	Ejemplo
Por sofisticación	**Script kiddies**	Individuos con pocos conocimientos que usan herramientas listas.	Uso de exploits descargados de internet
	Cibercriminales organizados	Grupos estructurados con fines económicos y recursos medios.	Ransomware-as-a-Service, mercados negros
	APT Groups	Actores avanzados, persistentes y con recursos casi ilimitados.	Operaciones de inteligencia o espionaje

4-Defensa en Profundidad

> Defensa en Profundidad

```
- Estrategia de seguridad por capas - si una falla, otras protegen
```

Capa	Descripción / Alcance	Controles típicos
Capa 1 - Física	Seguridad de las instalaciones y hardware físico.	Control de acceso, cámaras, guardias.
Capa 2 - Perimetral	Protección del borde de red.	Firewalls, IPS/IDS, VPN, segmentación de red.
Capa 3 - Red interna	Control del tráfico interno.	NAC, VLANs, microsegmentación.
Capa 4 - Endpoint	Protección de equipos y servidores.	Antimalware, EDR, hardening de SO.
Capa 5 - Aplicación	Seguridad del software y servicios.	WAF, validación de inputs, SAST/DAST.
Capa 6 - Datos	Protección de la información sensible.	Cifrado, DLP, clasificación.
Capa 7 - Humana	Concienciación y formación de usuarios.	Formación, concienciación, políticas.

> Cyber Kill Chain

```
- Es un marco de 7 fases que describe cómo avanza un ciberataque
```

Fase	Descripción	Ejemplo
Reconnaissance	Recopilación de información sobre el objetivo.	OSINT, escaneo de puertos, fingerprinting.
Weaponization	Creación de payload y exploit.	Construcción de malware o documento malicioso.
Delivery	Envío del arma al objetivo.	Email de phishing, USB, web maliciosa.
Exploitation	Ejecución del exploit en el sistema víctima.	Explotar una vulnerabilidad del SO o app.
Installation	Instalación de backdoor o malware persistente.	Implantar troyano, servicio oculto.
Command & Control (C2)	Comunicación con el servidor del atacante.	Canal cifrado hacia servidor C2.
Actions on Objectives	Ejecución del objetivo final del ataque.	Robo de datos, cifrado, sabotaje.

```
Objetivo defensivo: Romper la cadena en la fase más temprana posible
```

MITRE ATT & CK Framework
Base de conocimiento con todas las técnicas que se emplean en cada fase de las Cyber Kill Chain.

> Detección de Amenazas - IOCs
> **IOC (Indicator of Compromise):** Artefactos observables que sugieren que un sistema ha sido comprometido

Vector / Amenaza IOC	Explicación detallada	Medida(s) de defensa	Descripción de la defensa
IOC de red	IPs maliciosas, dominios C2, patrones de tráfico anómalos (beacons, exfiltración).	Threat intelligence feeds	Suscripciones a feeds de inteligencia de amenazas actualizados (VirusTotal, AlienVault OTX).
IOC de host	Hashes de malware (MD5/SHA256), nombres de archivos sospechosos, claves de registro.	EDR/SIEM	Endpoint Detection & Response y Security Information Event Management con IOC matching.
IOC de comportamiento	Procesos anómalos,	UEBA/Comportamiento Analytics	Análisis de patrones de usuario/entidad

Vector / Amenaza IOC	Explicación detallada	Medida(s) de defensa	Descripción de la defensa
	conexiones inusuales, accesos fuera de horario.		para detectar desviaciones del comportamiento normal.
Fuentes de IOC insuficientes	Falta de IOCs actualizados o mala correlación entre fuentes.	Honeypots + SIEM correlación	Sistemas trampa para atraer atacantes + correlación automática de eventos entre fuentes.

`5-Vectores de Ataque`

>Es el **camino o método** que usa un atacante para entrar en un sistema, red o aplicación y explotar una vulnerabilidad.

5.0 Superficie de Ataque

> **Definición:** Suma de todos los puntos de entrada posibles donde un atacante puede intentar comprometer un sistema

Tipo de superficie de ataque	Descripción breve
Superficie física	Acceso directo a hardware, puertos USB, servidores u otros componentes físicos del sistema.
Superficie digital	Exposición mediante aplicaciones web, APIs, servicios de red y endpoints conectados.
Superficie social	Riesgos asociados a empleados, contratistas o partners que pueden ser manipulados o cometer errores.

Hardening

Reducir la superficie de ataque significa minimizar los puntos por los cuales un atacante podría acceder o comprometer un sistema. El *hardening* (endurecimiento) consiste en aplicar técnicas y configuraciones que cierran o eliminan esas posibles vías de ataque.

Acción de hardening	Descripción breve
Deshabilitar servicios innecesarios	Desactiva funciones, protocolos o demonios que no se usan (por ejemplo, Telnet, FTP o puertos abiertos sin uso).

Acción de hardening	Descripción breve
Cerrar puertos no esenciales	Limita las conexiones solo a los puertos estrictamente necesarios para la operación del sistema.
Restringir accesos	Implementa control de acceso basado en roles (RBAC), autenticación fuerte y principio de mínimo privilegio.
Aplicar segmentación de red	Separa redes críticas de las redes de usuarios o de Internet mediante VLANs o firewalls.
Actualizar y parchear regularmente	Mantén firmware, sistemas operativos y aplicaciones al día para evitar vulnerabilidades conocidas.
Monitorear y auditar	Supervisa la actividad y los accesos para detectar comportamientos anómalos y comprobar el cumplimiento de políticas.

5.1 Superficie Física

5.1.1 Medios Extraíbles

Vector / Amenaza	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
USB malicioso	Autorun de malware, BadUSB (emula teclado para comandos)	Deshabilitar autorun	Impide ejecución automática de archivos al conectar USB	Evita malware que se ejecuta solo por insertar el dispositivo
		Bloqueo de USB por política	Restringe conexión de USB según usuario/dispositivo autorizado	Controla qué USBs pueden conectarse
		EDR	Detecta comportamientos anómalos como ejecución de comandos inusuales	Identifica BadUSB que emula dispositivos legítimos

Vector / Amenaza	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Rubber Ducky / Bash Bunny	USBs que ejecutan payloads/scripts automáticamente	Deshabilitar autorun	Impide ejecución automática de archivos al conectar USB	Bloquea payloads que dependen de ejecución automática
		EDR	Monitoriza escritura rápida	Detecta patrones característicos de

Vector / Amenaza	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
			de comandos (keystroke injection)	estos dispositivos
		Bloqueo de USB por política	Políticas que autorizan solo dispositivos USB conocidos	Previene conexión de dispositivos no identificados

Vector / Amenaza	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Baiting físico	USBs "perdidos" dejados para que empleados los conecten	Concienciación	Formación: nunca conectar USB desconocidos o encontrados	Reduce que empleados caigan en la trampa
		Bloqueo de USB por política	Prohíbe USBs no autorizados en sistemas críticos	Previene conexión incluso si el empleado lo intenta
		Escaneo antivirus	Analiza contenido de USBs autorizados antes de permitir ejecución	Detecta malware en USBs aparentemente "inofensivos"

5.2 Superficie Digital

5.2.1 Email

> Vector mas común

Vector / Amenaza de email	Explicación detallada	Medida(s) de defensa	Cómo ayuda
Adjuntos maliciosos	Archivos *.exe*, *.docm* con macros, *.pdf* con exploits o *.zip* con malware.	Sandboxing de adjuntos	Aísla y analiza archivos sospechosos antes de permitir su apertura.
Enlaces a sitios maliciosos	Links de *phishing* o descargas *drive-by* que	Gateway de correo con	Escanea y bloquea enlaces maliciosos

Vector / Amenaza de email	Explicación detallada	Medida(s) de defensa	Cómo ayuda
	infectan al hacer clic.	análisis de URLs	antes de que lleguen al usuario.
Spoofing de remitente	Suplantación del dominio o dirección de un remitente legítimo.	SPF, DKIM y DMARC	Verifica autenticidad del remitente y bloquea emails falsificados.
Business Email Compromise (BEC)	Compromiso de cuenta legítima para fraudes financieros o robos de información.	Entrenamiento antiphishing, MFA	Formación detecta intentos de ingeniería social; MFA protege cuentas.

5.2.2 Aplicaciones Web

Vector / Amenaza web	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Vulnerabilidades de aplicación	Fallos OWASP Top 10: SQLi, XSS, CSRF y otros que permiten comprometer el sistema.	WAF	Filtro que inspecciona tráfico HTTP/HTTPS para detectar y bloquear ataques web típicos.	Bloquea ataques en tiempo real.
Vulnerabilidades de aplicación	Fallos OWASP Top 10: SQLi, XSS, CSRF y otros que permiten comprometer el sistema.	SAST/DAST	Análisis estático/dinámico del código para identificar vulnerabilidades.	Detecta fallos antes y después del despliegue.
Vulnerabilidades de aplicación	Fallos OWASP Top 10: SQLi, XSS, CSRF y otros que permiten comprometer el sistema.	Secure SDLC	Seguridad integrada en todo el ciclo de vida del desarrollo.	Previene riesgos desde el diseño inici
Drive-by downloads	Malware se descarga automáticamente al visitar sitio comprometido.	Navegadores actualizados	Mantiene navegadores y extensiones parcheados	Cierra vulnerabilidad que permiten descargas automáticas.

Vector / Amenaza web	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
			contra exploits conocidos.	
Drive-by downloads	Malware se descarga automáticamente al visitar sitio comprometido.	Aislamiento de navegador	Ejecuta navegadores en entornos virtualizados o aislados.	Limita daño s malware se ejecuta.
Exploit kits	Frameworks automatizados que prueban múltiples vulnerabilidades del navegador/plugins.	Navegadores actualizados	Mantiene navegadores y extensiones parcheados contra exploits conocidos.	Protege contr kits que busc vulnerabilidad conocidas.
Exploit kits	Frameworks automatizados que prueban múltiples vulnerabilidades del navegador/plugins.	EDR	Monitoriza endpoints para detectar comportamientos anómalos e infecciones.	Respuesta rápida ante infecciones detectadas.
Watering hole	Compromiso de sitios legítimos frecuentados por objetivos específicos.	EDR	Monitoriza endpoints para detectar comportamientos anómalos e infecciones.	Detecta infecciones d sitios aparentemen legítimos.
Watering hole	Compromiso de sitios legítimos frecuentados por objetivos específicos.	Navegadores actualizados	Mantiene navegadores y extensiones parcheados contra exploits conocidos.	Reduce éxito ataques dirigidos a navegadores.

5.2.3 Redes Inseguras

> Permiten capturar tráfico no cifrado (páginas HTTP, algunas apps mal configuradas) y realizar ataques MITM para intentar descifrar o modificar comunicaciones

Vector / Riesgo de red	Explicación detallada	Medida(s) de defensa	Cómo ayuda
Escaneo de puertos	Identificación de servicios expuestos	Firewall, segmentación de	Limita puertos y segmentos visibles

Vector / Riesgo de red	Explicación detallada	Medida(s) de defensa	Cómo ayuda
	mediante Shodan, Masscan o Nmap.	red	desde el exterior.
Explotación de servicios vulnerables	Ataques contra SMB (EternalBlue), RDP o SSH con credenciales débiles.	IPS/IDS, deshabilitar legacy, parches	Bloquea exploits y elimina servicios/protocolos inseguros.
Redes públicas sin cifrado	WiFi abierta permite capturar tráfico no cifrado y facilitar MITM.	VPN con MFA	Cifra todo el tráfico del usuario en redes no confiables.
Man-in-the-Middle (MITM)	Atacante intercepta y modifica tráfico entre usuario y servidor.	VPN con MFA, monitorización	Protege datos y detecta anomalías en tiempo real.
Redes falsas (Evil Twin)	AP WiFi falso que imita red legítima para capturar tráfico.	VPN con MFA, concienciación usuario	VPN cifra datos; formación ayuda a identificar redes falsas.
WEP/WPA cracking	Rompe cifrados débiles WiFi para obtener acceso o credenciales.	WPA2/WPA3, contraseñas fuertes	Cifrados modernos resisten ataques de fuerza bruta y cracking.
VPN vulnerables	Exploits en Pulse Secure, Fortinet, Citrix para acceder a red interna.	VPN con MFA, hardening y actualizaciones	Reduce superficie de ataque y exige autenticación multifactor.
Movimiento lateral	Propagación de ataques dentro de la red tras compromiso inicial.	Segmentación de red, monitorización	Aísla zonas críticas y detecta tráfico anómalo entre segmentos.

5.2.4 Cloud

Vector / Amenaza Cloud	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Misconfiguración de buckets S3	Buckets configurados como públicos exponen millones de registros sin autorización.	CSPM	Monitoriza y corrige configuraciones inseguras en la nube automáticamente.	Detecta buckets públicos y aplica políticas de acceso correctas.
Credenciales comprometidas	API keys hardcodeadas	Secretos en vaults	Almacena credenciales en	Evita exposición accidental de

Vector / Amenaza Cloud	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
	en repositorios GitHub públicos o código fuente.		servicios seguros (AWS Secrets Manager, HashiCorp Vault).	claves en código o repos públicos.
Abuso de permisos IAM	Escalada de privilegios mediante políticas IAM mal configuradas o permisos excesivos.	IAM bien configurado	Aplica principio de menor privilegio y revisa permisos regularmente.	Limita el alcance de daño si credenciales se comprometen.
Vulnerabilidades en containers	Imágenes Docker con malware o vulnerabilidades conocidas sin parches.	Escaneo de containers	Analiza imágenes en repositorios y runtime para vulnerabilidades y malware.	Bloquea despliegue de containers inseguros.
Acceso no autorizado (general)	Cualquier brecha en configuraciones cloud que permita accesos externos.	Zero Trust	Nunca confía, siempre verifica identidad, contexto y postura de seguridad.	Protege contra accesos internos/externos no autorizados en cualquier escenario.

5.2.5 Vulnerabilidades de Software

> Errores o debilidades en el código que pueden ser explotados por atacantes

Vector / Amenaza Software	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Zero-day	Vulnerabilidades desconocidas por el proveedor, sin parche disponible.	EDR/Comportamiento Analytics	Monitoriza patrones anómalos que indican explotación de zero-days.	Detecta ataques sin firmas conocidas mediante heurística y ML.
Buffer overflow	Explotar memoria desbordada para	ASLR/DEP + W^X	Address Space Layout Randomization,	Dificulta explotación al

Vector / Amenaza Software	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
	ejecutar código malicioso arbitrario.		Data Execution Prevention, W^X policies.	randomizar memoria y prevenir ejecución de datos.
SQL Injection (SQLi)	Insertar comandos SQL maliciosos en formularios web para robar/manipular bases datos.	WAF + Prepared Statements	Web Application Firewall + usar consultas parametrizadas en código.	Bloquea payloads SQLi y previene inyección desde el diseño del código.
XSS (Cross-Site Scripting)	Inyectar scripts maliciosos en páginas web que se ejecutan en navegador de víctimas.	CSP + Input Sanitization	Content Security Policy + validar/sanitizar toda entrada de usuario.	Bloquea ejecución de scripts no autorizados y limpia inputs maliciosos.

5.2.6 Dispositivos Sin Actualizar

> Los parches de seguridad son críticos para corregir vulnerabilidades conocidas

Vector / Amenaza Sin Parches	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Sistemas operativos obsoletos	Windows XP, Linux sin support, vulnerables a exploits conocidos.	Patch Management Automatizado	WSUS, Ansible, SCCM para despliegue centralizado y automatizado de parches.	Cierra vulnerabilidades conocidas antes de que sean explotadas masivamente.
Software sin parches seguridad	Aplicaciones de terceros sin updates (Adobe Flash, Java antigua).	Inventario + Auto-update	Asset Management + políticas de auto-actualización obligatoria.	Identifica software desactualizado y fuerza updates.

Vector / Amenaza Sin Parches	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Firmware IoT nunca actualizado	Cámaras, routers con backdoors permanentes por falta de parches.	Network Segmentation + Air-gapping	VLANs dedicadas para IoT + aislamiento físico de dispositivos críticos.	Limita impacto si dispositivo IoT se compromete.
Ventana de oportunidad	Período entre publicación de vulnerabilidad y despliegue de parche.	Zero-day Protection + SBOM	EDR avanzado + Software Bill of Materials para conocer componentes vulnerables.	Mitiga exploits conocidos y trackea dependencias de software.

5.2.7 Contraseñas Débiles

Problema / Error común	Por qué es peligroso / Riesgo	Práctica recomendada	Beneficio / Cómo ayuda
123456, password	Fáciles de adivinar o crackear con diccionarios y ataques de fuerza bruta.	Mínimo 12 caracteres	Multiplica exponencialmente el tiempo de cracking.
Fechas de nacimiento	Información pública en redes sociales, fácil de adivinar.	Mezcla de caracteres	Mayúsculas, minúsculas, números, símbolos = combinaciones imposibles.
Nombres de mascotas	Datos personales fácilmente descubribles por OSINT.	Gestor de contraseñas	Genera y guarda contraseñas únicas automáticamente por sitio.
Misma contraseña múltiples sitios	Una filtración compromete **todas** las cuentas del usuario.	Autenticación multifactor (MFA)	Requiere "algo que tienes" además de la contraseña.

5.3 Superficie Social

5.3.1 Ingeniería Social

> Manipulación psicológica para que las personas revelen información confidencial

Técnica de ingeniería social	Explicación breve
Explotación de la confianza humana	Aprovechar la buena fe y confianza natural entre personas para obtener información o acceso.
Pretexting	Crear historias falsas creíbles para manipular a la víctima (ej: hacerse pasar por técnico de IT).
Baiting	Ofrecer algo irresistible (USB infectado, premio falso) para que la víctima lo active.
Tailgating	Seguir físicamente a alguien autorizado para entrar a zonas restringidas sin credenciales.

5.3.2 Amenazas Internas

> **Insider Threat:** Amenaza proveniente de personas con acceso legítimo (empleados, contratistas, partners)

Vector / Amenaza interna	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Empleados maliciosos	Empleado descontento roba/sabotea datos intencionalmente	Mínimos privilegios	Cada usuario solo accede a datos/funciones necesarias para su rol	Limita el daño que puede causar un insider malicioso
		DLP (Data Loss Prevention)	Monitoriza/bloquea transferencia de datos sensibles a destinos no autorizados	Detecta y previene exfiltración de información crítica

Vector / Amenaza interna	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Empleados negligentes	Error humano, mala configuración, phishing	Mínimos privilegios	Reduce impacto de errores limitando acceso y permisos del usuario	Un error no compromete toda la organización
		UEBA	Analiza patrones de comportamiento	Identifica cuando usuario "normal"

Vector / Amenaza interna	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
			para detectar anomalías en usuarios legítimos	actúa sospechosamente

Vector / Amenaza interna	Explicación detallada	Medida(s) de defensa	Descripción de la defensa	Cómo ayuda
Cuentas comprometidas	Credenciales robadas de empleado legítimo	UEBA	Detecta accesos inusuales (hora, ubicación, patrones) en cuentas legítimas	Distingue accesos legítimos de atacantes con credenciales robadas
		Offboarding seguro	Revoca inmediatamente accesos al salir de la organización	Evita que ex-empleados o cuentas comprometidas mantengan acceso

`6-Tipos de Amenazas Cibernéticas`

Clasificación de Ataques

Categoría	Subcategoría	Ejemplos de ataques
Por objetivo CIA	**Confidencialidad**	Espionaje, robo de datos
	Integridad	Modificación de datos, sabotaje
	Disponibilidad	DDoS, ransomware
Por tipo de activo	**Red**	MITM, sniffing, spoofing
	Aplicación	Inyecciones SQL, XSS
	Sistema	Malware, rootkits
	Humano	Ingeniería social (phishing, vishing)

6.1 Ataques por Vector

6.1.1 Malware

> **Software malicioso** diseñado para dañar, explotar o comprometer sistemas

Comparativa Completa de Malware

Tipo	Cómo entra	Qué hace	Objetivo	Detección
Virus	Acción usuario (abrir archivo)	Infecta archivos/ejecutables	Replicarse en archivos	Firmas, heurísti
Gusano	Vulnerabilidades red	Se replica SOLO por red	Saturar redes	IDS, tráfico anómalo
Troyano	Engaño (falsa app)	Abre **puerta trasera** (RAT)	Acceso remoto	Análisis comportamenta
Ransomware	Phishing/RDP/vulns	**Cifra archivos** + publica datos	Dinero (rescate)	Backups, EDR
Spyware	Engaño (keyloggers)	**Roba datos silenciosamente**	Información sensible	Análisis memoria/proce
Adware	Descargas dudosas	**Anuncios infinitos** + ralentiza	Generar ingresos pubs	Anti-adware, limpieza nav
Rootkit	Exploit/vulns	**Se esconde en KERNEL**	Control total invisible	Boot limpio, análisis RAM
Botnet	Infección masiva	**Controla MILLONES dispositivos**	DDoS, spam, minado	C2 traffic, comportamient

Virus

> **Definición:** Software malicioso que se adjunta a archivos legítimos y se replica infectando otros archivos cuando se ejecuta

Característica	Descripción
Ejecución	Requiere acción del usuario (abrir archivo infectado)
Propagación	Medios extraíbles, adjuntos email, descargas web
Tipos	Boot sector virus, Macro virus, File infector virus
Detección	Firmas antivirus, análisis heurístico, sandboxing

Gusanos (Worms)

> **Definición:** Malware autorreplicante que se propaga automáticamente por la red sin intervención humana

Característica	Descripción
Archivo host	No necesita archivo host - se propaga por sí mismo
Propagación	Explota vulnerabilidades de red para infectar sistemas
Impacto en red	Puede saturar redes con tráfico de replicación
Velocidad	Propagación exponencial - miles de sistemas en minutos

Troyanos (Trojans)

> **Definición:** Malware que se disfraza de software legítimo para engañar al usuario y obtener acceso al sistema

Característica	Descripción
Autoreplicación	No se autorreplica - se instala por engaño
Funcionalidad	Crea backdoors para acceso remoto (RAT)
Capacidades	Keylogging, captura de pantalla, robo de credenciales, descarga de más malware

Ransomware

> **Definición:** Malware que cifra archivos del sistema y exige rescate económico (generalmente en criptomonedas) para descifrarlos

Característica	Descripción
Táctica	Doble extorsión: Cifrado + amenaza de publicar datos robados
Modelo de negocio	Ransomware-as-a-Service (RaaS)
Impacto económico	Rescate medio: 200k-2M € (según sector)
Vectores de entrada	Phishing, RDP expuesto, vulnerabilidades sin parchear

Spyware

> Software que recopila información del usuario sin su conocimiento
> -Se instalan por engaño (como troyanos) y **roban información sensible** de forma silenciosa:

Tipo	Función principal	Qué roba
Keyloggers	Capturan pulsaciones de teclado	Contraseñas, datos bancarios

Tipo	Función principal	Qué roba
Screen scrapers	Capturan contenido de pantalla	Todo lo visible en pantalla
Stalkerware	Monitorización completa de móviles	GPS, SMS, llamadas, micrófono (teléfonos)

Adware

> Muestra anuncios no deseados, a menudo rastreando comportamiento
> -Se instala por descargas dudosas o bundles y **te bombardea con anuncios** para generar ingresos

Característica	Descripción	Impacto
Ventanas emergentes	Publicidad invasiva constante (pop-ups infinitos)	Interrupción constante del trabajo
Redirecciones	Navegador cambia páginas sin control	Redirige a webs maliciosas/phishing
Rendimiento	Ralentización del sistema	Consume CPU/memoria innecesariamente

Rootkits

> **Definición:** Malware que obtiene acceso privilegiado al sistema y se oculta modificando el sistema operativo

Característica	Descripción
Nivel kernel	Se integra en el núcleo del SO, máximo control
Stealth	Oculta procesos, archivos, conexiones de red, claves de registro
Persistencia	Sobrevive a reinicios y es difícil de detectar/eliminar
Detección	Análisis de memoria, boot desde medio limpio, UEFI Secure Boot

Botnets

> **Definición:** Red de dispositivos infectados (bots/zombies) controlados remotamente por un atacante (botmaster)

Característica	Descripción
Usos principales	DDoS, spam masivo, minado criptomonedas, ataques distribuidos
Tamaño	Miles a millones de dispositivos (PCs, IoT, routers)

Característica	Descripción
C2 (Control)	IRC, HTTP, P2P, dominios generados algorítmicamente (DGA)

6.1.2 Phishing

> Técnica de **INGIENERIA SOCIAL** que suplanta identidades legítimas para engañar a víctimas y robar información sensible (credenciales, datos bancarios)

Tipo de phishing	Significado	Explicación
Email phishing	Correos fraudulentos	Se envían correos falsos que imitan a empresas o servicios legítimos para engañar al usuario y obtener contraseñas, datos bancarios u otra información sensible.
Spear phishing	Ataques dirigidos	Variante más personalizada: los atacantes investigan previamente a la víctima y envían mensajes adaptados para parecer más creíbles.
Whaling	Objetivos de alto perfil	Forma de *spear phishing* dirigida a altos ejecutivos, directores o figuras con acceso a información crítica o recursos financieros.
Vishing	Phishing por llamadas telefónicas	El atacante llama haciéndose pasar por una entidad legítima (banco, soporte técnico) para obtener datos personales o bancarios.
Smishing	Phishing por SMS	Se envían mensajes de texto con enlaces falsos o alertas engañosas que buscan que el usuario entregue información o instale malware.

6.1.3 Ataques de Red

6.1.3.1 Man-in-the-Middle (MITM)

> Atacante se posiciona entre dos partes que se comunican para interceptar, leer o modificar el tráfico

Técnica	Descripción
ARP Spoofing	Envenenar caché ARP para redirigir tráfico a atacante
DNS Spoofing	Respuestas DNS falsas redirigen a sitios maliciosos
Session hijacking	Robo de cookies/tokens de sesión activa
SSL Stripping	Degradar HTTPS → HTTP para leer tráfico en claro

6.1.3.2 Ataques DDoS

> **Distributed Denial of Service:** Saturación de recursos de un sistema/red con tráfico masivo desde múltiples fuentes para dejarlo inaccesible

Tipo de DDoS	Descripción	Elementos clave
Volumétricos	Saturación de ancho de banda	**Redes botnet**, **Dispositivos IoT**
De protocolo	Agotar recursos del servidor	**Redes botnet**, **Interrupción servicios**
De aplicación (L7)	Peticiones HTTP masivas/lentas	**Redes botnet**, **Chantaje/extorsión**

Elemento del ataque DDoS	Descripción
Redes botnet	Conjunto de dispositivos infectados que envían solicitudes simultáneamente al objetivo.
Interrupción de servicios críticos	Los servidores o aplicaciones dejan de funcionar, afectando operaciones empresariales.
Chantaje ("Paga o seguimos atacando")	Extorsión en la que los atacantes exigen dinero para detener el ataque.
Dispositivos IoT vulnerables	Aparatos conectados a Internet (como cámaras o routers) usados sin conocimiento del dueño para generar tráfico de ataque.

6.2 Ataques Avanzados

6.2.1 Inyección SQL

> Inserción de código SQL malicioso en inputs de aplicación web para manipular la base de datos

Tipo de impacto	Descripción	Ejemplo
Extracción de datos	Dump completo de bases de datos	`SELECT * FROM users`
Bypass autenticación	Acceso sin credenciales válidas	`' OR '1'='1' --`
Modificación/borrado	Alterar o eliminar datos/tablas	`DROP TABLE users; UPDATE`
Ejecución comandos	Remote Code Execution (RCE) en servidor	`xp_cmdshell 'net user hacker'`

6.2.2 Cross-Site Scripting (XSS)

> Inyección de scripts maliciosos (JavaScript) en páginas web vistas por otros usuarios

Tipo	Cómo funciona	Ejemplo
Reflected XSS	Script en URL, ejecuta al hacer clic en enlace	`?search=<script>alert('hack')</script>`
Stored XSS	Script guardado en servidor (foro/comentarios)	`<script>stealCookies()</script>` en perfil
DOM-based XSS	Manipula DOM directamente en navegador del cliente	`document.location=malicious.com`

Consecuencia	Descripción
Robo sesiones	Cookies/tokens robados
Keylogging	Captura pulsaciones en páginas atacadas
Redirección	Víctima enviada a phishing
Desfiguración	Web vandalizada (defacement)

6.2.3 Ataques Web Avanzados

Ataque	Descripción	Ejemplo práctico	Impacto
CSRF	Forzar usuario **autenticado** a ejecutar acciones no deseadas	`<img src="banco.com/transferir?cuenta=atacante&monto=1000">`	Transferencias, cambio contraseña, borrar datos
XXE	Explotar parsers **XML mal configurados** para leer archivos o SSRF	`<!ENTITY xxe SYSTEM "file:///etc/passwd">`	Lectura `/etc/passwd`, SSRF, RCE potencial
SSRF	Hacer que **servidor** haga peticiones a recursos internos/externos no autorizados	`http://169.254.169.254/latest/meta-data/` (AWS metadata)	Acceso red interna, cloud metadata, pivoteo

6.2.4 Ataques a Credenciales

Ataque	Descripción	Ejemplo
Brute Force	Probar **todas las combinaciones posibles** de contraseña	`aaa, aab, aac... zzz`
Dictionary Attack	Probar contraseñas **comunes de diccionarios**	`123456, password, qwerty`
Credential Stuffing	Usar credenciales **robadas de otras brechas** (reutilización)	`user@gmail.com:123456` de LinkedIn
Password Spraying	Probar **1 contraseña común contra MUCHOS usuarios** (evita bloqueos)	`Summer2024` en todos los AD users
Rainbow Tables	**Hashes precalculados** para revertir hashes rápidamente	MD5 `5f4dcc3b` : `password`
Pass-the-Hash	Usar **hash de contraseña directamente** sin descifrarla	`NTLM hash` para acceso lateral

Defensa	Cómo funciona
MFA (Multifactor)	Requiere 2+ factores, bloquea 99% ataques creds
Rate Limiting	Limita intentos por IP/usuario (ej: 5/minuto)
CAPTCHA	Bloquea automatización
Salting + Hash fuerte	`bcrypt` , `Argon2` + salt único por usuario
Monitorización	Alertas en intentos fallidos masivos
Políticas fuertes	Mínimo 12 chars, sin reutilización, sin comunes

6.2.5 APT - Amenazas Persistentes Avanzadas

>**Ataques cibernéticos altamente sofisticados** y generalmente **patrocinados por estados o grandes organizaciones criminales**.

- Su característica principal es la **PERSISTENCIA**:
- los atacantes permanecen dentro de la red de la víctima durante largos periodos sin ser detectados, recopilando información sensible y controlando sistemas clave.

Característica	Descripción	Ejemplo
Altamente dirigidos	Objetivos específicos: gobiernos, corporaciones críticas, infraestructuras	Ministerio Defensa, empresas energía
Recursos ilimitados	Estados-nación financian operaciones con presupuesto militar	Equipos dedicados 24/7
Técnicas avanzadas	Zero-days, custom malware, living-off-the-land	Herramientas legítimas mal usadas

Característica	Descripción	Ejemplo
Persistencia larga	Meses/años infiltrados sin detección	2+ años en red corporativa
Fases del ataque	Recon → Compromiso → Foothold → Escalada → Lateral → Misión	Kill Chain extendida

Aspecto	Descripción
Objetivos alto valor	Gobiernos, corporaciones estratégicas, sectores críticos
Ataques prolongados	Infiltración silenciosa durante meses/años
Robo estratégico	Datos confidenciales, propiedad intelectual, secretos de estado
Espionaje industrial	Ventaja tecnológica/geopolítica
Actores 2026	**Grupos chinos lideran** actividad APT (análisis globales)

```
1 RECONNAISSANCE → OSINT exhaustivo
2 COMPROMISO INICIAL → Spearphishing/zero-day
3 ESTABLECER FOOTHOLD → Custom malware sigiloso
4 ESCALADA PRIVILEGIOS → Credenciales robadas
5 MOVIMIENTO LATERAL → Red interna completa
6 MISIÓN → Exfiltración silenciosa datos
```

6.2.6 Ataques a la Cadena de Suministro

> Comprometer proveedores o software de terceros para infectar múltiples objetivos

Elemento / Tipo de ataque	Descripción breve
Software supply chain	Inyectar malware en actualizaciones legítimas de software utilizado por miles de organizaciones.
Hardware supply chain	Chips maliciosos insertados en dispositivos durante fabricación (ej. backdoors en firmware).
Servicios de terceros	Comprometer proveedores SaaS/cloud para atacar a todos sus clientes simultáneamente.
Compromiso de proveedores	Atacar empresas externas para usarlas como puente hacia el objetivo principal.
Compromiso de software de terceros	Manipular actualizaciones o componentes que muchas organizaciones integran.
Inyección de código en librerías open source	Alterar bibliotecas públicas (ej. npm, PyPI) que se integran en productos finales.
Efecto multiplicador	Un solo compromiso impacta a toda la cadena de clientes/proveedores conectados.

6.2.7 Amenazas IoT y OT

> **Internet of Things (IoT):** Dispositivos conectados con seguridad frecuentemente débil - cámaras, routers, termostatos, sensores industriales

Tipo de amenaza IoT/OT	Descripción breve
Superficie de ataque en expansión	Cada vez más dispositivos conectados aumentan los puntos vulnerables.
Dispositivos sin protección	Cámaras, sensores y otros equipos con poca o nula seguridad incorporada.
Ataques a infraestructuras críticas	Riesgo para sistemas de agua, energía, transporte u otros servicios esenciales.
Sectores industriales en riesgo	Manufactura, salud y logística expuestos a paradas, sabotaje o manipulación de datos.
Credenciales por defecto	Uso de combinaciones como *admin/admin* que no se cambian y facilitan accesos no autorizados.
Firmware sin actualizar	Dispositivos con versiones antiguas con vulnerabilidades conocidas sin parchear.
Protocolos inseguros	Uso de Telnet, HTTP sin cifrar o MQTT sin autenticación que exponen datos sensibles.
Botnets IoT	Redes de dispositivos comprometidos (ej. Mirai) usadas para ataques DDoS masivos.

6.3 Tendencias 2026

6.3.1 Deepfakes e IA Maliciosa

> Uso de inteligencia artificial para crear contenido falso hiperrealista

Amenaza basada en IA	Descripción breve
Videos falsos	Deepfakes usados para suplantar a ejecutivos y cometer fraudes.
Voz sintética	Imitación de voces reales en llamadas fraudulentas para engañar a víctimas.
Malware adaptativo	Programas maliciosos con IA que cambian su comportamiento para evadir defensas en tiempo real.
Campañas de desinformación	Uso de IA para crear y difundir noticias falsas o manipular la opinión pública.

6.3.2 WhatsApp: Vector de Ataque 2026

> Las plataformas de mensajería instantánea, especialmente **WhatsApp**, se han convertido en un **canal prioritario para los ciberdelincuentes**. Esto se debe a la enorme cantidad de usuarios activos, la confianza entre contactos y la facilidad con que se pueden compartir archivos y enlaces.

Vector de ataque	Descripción breve
Troyanos mediante mensajes falsos	Enlaces o archivos falsos instalan un troyano con acceso remoto al dispositivo.
Suplantación de identidad masiva	Imitan contactos reales para engañar y robar datos o dinero.
Propagación viral de malware	Los usuarios reenvían sin saberlo mensajes maliciosos, expandiendo la infección.
Explotación de confianza entre contactos	Los criminales se aprovechan de la confianza en los contactos para difundir fraudes o spyware.

6.3.3 Ataques Basados en Identidad

> En lugar de atacar directamente los sistemas, los ciberdelincuentes **se infiltran usando identidades legítimas**, lo que les permite moverse dentro de las redes sin levantar sospechas.
> Este tipo de ataques combina ingeniería social, phishing avanzado e inteligencia artificial.

Vector de ataque relacionado con identidad	Descripción breve
Robo de credenciales	Obtención de contraseñas robadas o filtradas para acceder a sistemas sin autorización.
Identidades no humanas (NHI)	Uso o manipulación de cuentas de servicio, APIs o bots automatizados como punto de entrada.
Movimiento lateral	Expansión dentro de la red tras obtener acceso inicial, buscando mayores privilegios o datos.
Abuso de tokens	Secuestro de sesiones activas mediante el uso indebido de tokens de autenticación.

`7-Estrategias de Protección`

7.1 Prevención Básica

7.1.1 Firewalls

> Barrera de seguridad que filtra el tráfico entre redes según reglas predefinidas

Tipo de Firewall	Función principal
Firewall de red	Filtra tráfico por IP, puertos y protocolos entre redes.
Firewall de aplicación (WAF)	Protege aplicaciones web bloqueando ataques como SQL injection o XSS.
Next-Gen Firewall (NGFW)	Combina todas las funciones + inspección profunda de paquetes y detección de amenazas avanzadas.

Función	Descripción
Bloquear tráfico malicioso	Detiene paquetes sospechosos según reglas predefinidas.
Inspección de paquetes	Analiza contenido de datos (no solo cabeceras) para detectar amenazas.
Prevención de intrusiones	Identifica y bloquea ataques en tiempo real usando firmas de amenazas conocidas.

7.1.2 Antivirus y Antimalware

> Programas que **buscan, bloquean y eliminan virus y malware** para proteger tu ordenador, móvil o red de ataques.

Función de Antivirus	Descripción breve
Detección por firmas	Compara archivos con base de datos de malware conocido.
Análisis heurístico	Detecta comportamientos sospechosos aunque no esté en la base de datos.
Sandboxing	Ejecuta archivos dudosos en entorno aislado para observar su comportamiento.
Protección en tiempo real	Monitorea continuamente el sistema y bloquea amenazas al instante.
Actualización constante	Descarga diariamente nuevas firmas de amenazas y patrones de ataque.

7.2 Control de Acceso

7.2.1 Modelo Zero Trust

> **Principio:** "Nunca confíes, siempre verifica"
> Ningún usuario o dispositivo es confiable por defecto

Componente	Explicación breve
Verificación continua de identidad	Comprueba constantemente quién eres, desde dónde accedes y si sigues siendo confiable.
Acceso basado en contexto y riesgo	Evalúa ubicación, hora, dispositivo, comportamiento antes de permitir acceso (ej: bloquea login desde Rusia a las 3AM).
Microsegmentación de redes	Divide la red en zonas pequeñas aisladas. Si comprometen una, no pueden moverse lateralmente.
Estándar consolidado en 2026	Modelo Zero Trust obligatorio para nubes híbridas por regulaciones y mejores prácticas.
Reemplazo de VPNs tradicionales	Las VPN dan acceso total una vez conectadas. Zero Trust da acceso granular y temporal.

7.2.2 Autenticación Multifactor (MFA)

> Requerir múltiples formas de verificación para acceder a un sistema

Factor de autenticación	Descripción breve	Ejemplos
Algo que sabes	Conocimiento que solo tú conoces	Contraseña, PIN, respuesta de seguridad
Algo que tienes	Objeto físico o dispositivo en tu posesión	Token USB, móvil (app autenticadora), tarjeta inteligente
Algo que eres	Característica biométrica única de tu cuerpo	Huella dactilar, reconocimiento facial, escáner de iris

7.3 Seguridad de Red

7.3.1 VPN y SASE

VPN Tradicional

Característica VPN Tradicional	Definición	Ejemplo práctico
Túnel cifrado	Crea un canal seguro en Internet que cifra todos los datos entre tu dispositivo y el servidor VPN	Tu tráfico de Netflix viaja cifrado desde tu casa hasta el servidor VPN en EE.UU.
Oculta dirección IP	Reemplaza tu IP real por la IP del servidor VPN, haciendo	Ves contenido bloqueado geográficamente (Disney+ USA desde España)

Característica VPN Tradicional	Definición	Ejemplo práctico
	imposible rastrear tu ubicación real	
Acceso remoto seguro	Conecta a redes corporativas como si estuvieras físicamente en la oficina	Empleado conecta desde casa a servidores internos de la empresa
En declive gradual	Reemplazada por Zero Trust y SASE por dar acceso total una vez conectado	Modelos modernos verifican continuamente identidad y contexto

SASE (2026)

> Es **seguridad + red todo-en-uno en la nube**.

Característica SASE	Definición	Ejemplo práctico
Secure Access Service Edge	Arquitectura que combina red y seguridad en la nube	Zscaler, Cato Networks: todo gestionado desde la nube
Convergencia red + seguridad	Une SD-WAN (red), FWaaS (firewall), ZTNA (Zero Trust) en una sola plataforma	Una suscripción incluye firewall, VPN y optimización WAN
Basado en la nube	Servicios distribuidos globalmente, sin hardware local	Acceso seguro desde cualquier ubicación sin appliances físicos
Futuro del acceso seguro	Reemplaza VPN + firewalls tradicionales para trabajo híbrido	Empleados remotos acceden solo a apps específicas sin VPN completa

7.3.2 Segmentación de Redes

> Dividir la red en zonas aisladas para limitar el movimiento lateral

Concepto	Definición	Beneficio clave
Dividir red en zonas aisladas	Separar red en compartimentos seguros	Atacante en "ventas" no llega a "finanzas"
Contener alcance de brecha	Limitar propagación si hay compromiso	Infectan 1 servidor → no afecta resto de red
Microsegmentación granular	Políticas de acceso por aplicación/servicio	Workload1 solo habla con Workload2, nada más
Separar entornos	Prod/Dev/DMZ aislados entre sí	Desarrolladores no acceden producción

Concepto	Definición	Beneficio clave
VLANs y subredes estrictas	Segmentación L2/L3 + políticas firewall	Tráfico solo permitido explícitamente

7.4 Detección y Respuesta

7.4.1 IDS/IPS

> Sistemas para detectar y prevenir intrusiones en tiempo real (Cámara de seguridad)

Sistema	Función principal	Diferencia clave
IDS (Detection)	Detecta y alerta sobre amenazas	Solo **avisa** (no actúa)
IPS (Prevention)	Detecta **y bloquea** amenazas	**Actúa automáticamente**
Análisis de tráfico anómalo	Identifica patrones de comportamiento sospechoso	Detecta ataques zero-day
Integración con SIEM	Correlaciona eventos con otros sistemas de seguridad	Contexto completo de incidentes

7.4.2 SIEM y SOC

> **SIEM y SOC** son los **"cerebros" de la ciberseguridad** de una empresa:
> SIEM es el **software** que recopila y analiza datos
> SOC es el **equipo humano** que responde 24/7.

Característica SIEM	Descripción
Agregación de logs	Recopila datos de todos los sistemas (firewalls, servidores, apps) en un lugar central.
Correlación de eventos	Une alertas aisladas para detectar ataques complejos que pasan desapercibidos.
Alertas en tiempo real	Notifica inmediatamente sobre amenazas críticas para respuesta rápida.

Característica SOC	Descripción
Equipo de analistas	Expertos humanos que investigan y responden a las alertas del SIEM.
Monitoreo 24/7	Supervisión continua, nunca duerme.
Respuesta a incidentes	Contención, eliminación de amenazas y recuperación de sistemas.

7.5 Protección de Datos

7.5.1 Cifrado

> Transformar información en un formato ilegible sin la clave correcta

Tipo de cifrado	Definición	Detalles técnicos
Simétrico	Usa **misma clave** para cifrar y descifrar	- AES (Advanced Encryption Standard): 128/192/256 bits - Muy rápido para grandes volúmenes de datos - Problema: cómo compartir la clave de forma segura
Asimétrico	Usa **par de claves**: pública (cifrar) + privada (descifrar)	- RSA: Basado en factorización de números primos grandes - Más lento, usado para intercambios seguros de claves - Firma digital (clave privada firma, pública verifica)
HTTPS (SSL/TLS)	Cifrado web que protege sitios HTTP	- Combina simétrico (datos) + asimétrico (intercambio de claves) - Certificados digitales verifican identidad del sitio - Candado 🔒 en navegador = conexión cifrada
Amenaza cuántica	Computadoras cuánticas rompen cifrado actual	- Algoritmo de Shor rompe RSA/EC en segundos - AES-256 resiste ataques cuánticos conocidos - NIST estandariza criptografía post-cuántica (2026)

7.6 Resiliencia

7.6.1 Backups y Recuperación

> Regla 3-2-1 -> Protege contra ransomware, fallos de hardware y desastres físicos.
> **3 copias totales** de tus datos,
> en **2 medios diferentes**,
> con **1 copia fuera de tu ubicación** (offsite).

Concepto	Definición	Detalles clave
Regla 3-2-1	3 copias, 2 tipos medios, 1 offsite	Ej: Disco local + NAS + nube (AWS S3 Glacier)
Backups inmutables	Copias que ransomware NO puede cifrar	Almacenadas en "solo lectura" o con retención fija
Pruebas regulares	Verificar que backups realmente restauran	Test trimestral: restaurar 10 archivos críticos
RTO (Recovery Time Objective)	Tiempo máximo aceptable de inactividad	"Máximo 4 horas sin email corporativo"
RPO (Recovery Point Objective)	Pérdida máxima de datos aceptable	"Máximo 1 hora de datos perdidos"

7.6.2 Gestión de Parches

> La **gestión de parches** es **actualizar software y sistemas** para cerrar **vulnerabilidades conocidas**.
> **No parchear = dejar la puerta abierta** con el cartel "Entra quien quiera".

Paso proceso	Definición	Importancia clave
Inventario completo activos	Lista de TODOS los sistemas, apps, dispositivos	Sin saber qué tienes, no puedes parchearlo
Priorización criticidad	Parchear primero lo más peligroso/expuesto	CVE crítico en servidor web > app interna poco usada
Automatización posible	Herramientas que actualizan sin intervención manual	WSUS, SCCM, Ansible: 90% automatizado
Verificación post-parche	Confirmar que parche se instaló y funciona	Reinicio OK + test funcionalidad crítica

7.7 Futuro 2026

7.7.1 IA en Ciberseguridad

> **La IA en ciberseguridad** es la **nueva frontera de la guerra digital en 2026**: sistemas autónomos que **defienden y atacan** automáticamente, analizando patrones imposibles para humanos.

Aspecto IA Ciberseguridad	Definición	Detalles clave
IA agéntica autónoma	Sistemas IA que toman decisiones sin intervención humana	Defiende redes automáticamente, responde a ataques en milisegundos
Defensa: Detección anomalías	IA que aprende comportamiento normal y alerta lo anómalo	Detecta insider threats, zero-days que humanos no ven
UEBA (User Entity Behavior Analytics)	Análisis de comportamiento de usuarios y entidades	"Juan nunca accede al servidor de finanzas a las 3AM desde Rusia"
Amenaza: IA maliciosa	Malware con IA que muta constantemente para evadir antivirus	Cambia su firma cada 5 minutos, aprende de sandbox
Carrera armamentista IA vs IA	Defensores y atacantes usan IA en competencia constante	Antivirus IA vs malware IA: evolución darwiniana digital