# **🔐 TEMARIO PARA CIBERSEGURIDAD**

## **🔰 NIVEL 0: INTRODUCCIÓN A LA CIBERSEGURIDAD**

### **1. Fundamentos de Ciberseguridad**

* ¿Qué es la ciberseguridad?
* Principales amenazas cibernéticas (malware, phishing, ransomware, etc.)
* Conceptos clave:  
  + Confidencialidad, integridad y disponibilidad (Triada CIA)
  + Autenticación y autorización
  + Riesgo y vulnerabilidades

### **2. Tipos de Amenazas Cibernéticas**

* **Malware**: Virus, troyanos, gusanos, rootkits
* **Phishing** y ataques de ingeniería social
* **Ransomware**: cómo funciona y cómo prevenirlo
* **Denegación de servicio (DoS) y DDoS**
* **Spyware** y **adware**
* **Exploits de vulnerabilidades** (zero-day)

### **3. Herramientas Básicas de Ciberseguridad**

* **Antivirus** y antimalware
* **Firewall** (cortafuegos)
* **Sistemas de detección y prevención de intrusos (IDS/IPS)**

## **🧱 NIVEL 1: FUNDAMENTOS DE REDES Y SEGURIDAD DE REDES**

### **4. Fundamentos de Redes**

* ¿Qué es una red? Tipos de redes (LAN, WAN, VPN, etc.)
* **Modelo OSI** y capas de red
* **Protocolos de red**:  
  + TCP/IP, UDP
  + HTTP, HTTPS, FTP, DNS, SMTP
* Direccionamiento IP (IPv4, IPv6) y subredes
* **Routers**, **switches**, **firewalls** y otros dispositivos de red

### **5. Seguridad de Redes**

* **Firewalls**: tipos y configuraciones
* **Seguridad en las comunicaciones**:  
  + Cifrado SSL/TLS
  + VPNs (Redes Privadas Virtuales)
  + Autenticación multifactor (MFA)
* **Seguridad de redes inalámbricas** (WPA2, WPA3, seguridad de redes WiFi)
* **Seguridad en aplicaciones web**: Protección contra XSS, SQL Injection, CSRF

## **⚙️ NIVEL 2: CRIPTOGRAFÍA Y PROTECCIÓN DE DATOS**

### **6. Fundamentos de Criptografía**

* Conceptos básicos:  
  + Cifrado simétrico vs. cifrado asimétrico
  + Algoritmos de cifrado: AES, RSA, DES, ECC
  + Funciones hash (SHA-256, MD5, etc.)
  + Certificados SSL/TLS
* **Cifrado de comunicaciones**: HTTPS, SSH, VPN
* **Firma digital** y **autenticación de mensajes**

### **7. Protección de Datos**

* **Políticas de protección de datos** y privacidad (GDPR, CCPA)
* **Cifrado de datos en reposo y en tránsito**
* **Gestión de contraseñas**: Hashing, salting y almacenamiento seguro de contraseñas
* **Backup y recuperación ante desastres**

## **🛡️ NIVEL 3: SEGURIDAD EN SISTEMAS Y APLICACIONES**

### **8. Seguridad en Sistemas Operativos**

* **Linux**: Seguridad en distribuciones (Ubuntu, Kali Linux, etc.), configuración de permisos, SELinux
* **Windows**: Políticas de seguridad, hardening de Windows Server
* **Hardening de sistemas**:  
  + Eliminación de servicios innecesarios
  + Parcheo de vulnerabilidades
  + Configuración de contraseñas seguras
* **Control de acceso**: ACLs (Access Control Lists), RBAC (Role-Based Access Control)

### **9. Seguridad en Aplicaciones Web**

* **OWASP Top 10**:  
  + Inyección SQL, Cross-Site Scripting (XSS), CSRF (Cross-Site Request Forgery)
  + Exposición de datos sensibles, control de acceso roto, configuración incorrecta de seguridad
* **Pruebas de penetración (pentesting)** en aplicaciones web
* **Frameworks de seguridad**: OWASP ZAP, Burp Suite
* **Autenticación y autorización**: OAuth, JWT, OpenID Connect
* **Protección contra vulnerabilidades en APIs** (REST, GraphQL)

## **🧠 NIVEL 4: CIBERSEGURIDAD EN LA NUBE Y SEGURIDAD MÓVIL**

### **10. Seguridad en la Nube**

* **Conceptos clave**: IaaS, PaaS, SaaS
* **Proveedores de servicios en la nube**: AWS, Azure, Google Cloud
* **Modelos de seguridad**: Shared Responsibility Model
* **Seguridad en entornos multicloud y híbridos**
* **Control de acceso en la nube**: IAM (Identity and Access Management)
* **Cifrado en la nube**: protección de datos en reposo y en tránsito

### **11. Seguridad en Dispositivos Móviles**

* **Protección de aplicaciones móviles**: Análisis de seguridad en apps iOS y Android
* **Autenticación** y **autorización** en apps móviles
* **Seguridad en redes móviles**: VPNs, Wi-Fi protegido
* **Protección contra malware** en dispositivos móviles
* **Políticas de seguridad móvil** y MDM (Mobile Device Management)

## **🧩 NIVEL 5: HACKING ÉTICO Y PRUEBAS DE PENETRACIÓN (PENTESTING)**

### **12. Pentesting: Pruebas de Penetración**

* **Reconocimiento (Reconnaissance)**: Reconocimiento pasivo y activo
* **Escaneo de vulnerabilidades**: Herramientas como Nmap, Nessus, OpenVAS
* **Explotación de vulnerabilidades**: Metasploit, Armitage
* **Escalada de privilegios**: Técnicas para obtener acceso a sistemas
* **Exfiltración de datos**: Técnicas para robar información de sistemas comprometidos

### **13. Red Teaming y Blue Teaming**

* **Red Teaming**: Simulación de ataques para probar defensas de la organización
* **Blue Teaming**: Defensa ante ataques, monitoreo de redes y detección de intrusos
* **Ciberataques simulados**: Análisis de incidentes y reportes

## **🕵️‍♂️ NIVEL 6: GESTIÓN DE INCIDENTES Y CUMPLIMIENTO**

### **14. Gestión de Incidentes de Seguridad**

* **Planes de respuesta ante incidentes**: Identificación, contención, erradicación, recuperación
* **Análisis forense digital**: Recuperación y análisis de datos tras un ataque
* **Herramientas forenses**: Autopsy, FTK Imager
* **Análisis de malware**: Descompilación, análisis de comportamiento

### **15. Cumplimiento de Normativas y Estándares de Seguridad**

* **ISO/IEC 27001**: Sistema de gestión de seguridad de la información
* **NIST Cybersecurity Framework**
* **GDPR**: Regulación de protección de datos personales
* **PCI-DSS**: Estándar de seguridad de datos en la industria de tarjetas de pago

## **🚀 NIVEL 7: CIBERSEGURIDAD AVANZADA Y TENDENCIAS EMERGENTES**

### **16. Ciberseguridad en IoT (Internet of Things)**

* **Riesgos y vulnerabilidades en dispositivos IoT**
* **Seguridad en redes IoT**: Configuración de redes y autenticación
* **Ataques comunes en IoT**: Botnets, inyección de comandos

### **17. Seguridad en Inteligencia Artificial y Machine Learning**

* **Riesgos y amenazas en AI/ML**
* **Ataques adversarios en modelos de ML**
* **Defensas y mitigación** de riesgos en AI

### **18. Blockchain y Criptomonedas: Seguridad**

* **Principios de seguridad en Blockchain**
* **Ataques a Blockchain**: 51% Attack, Sybil Attack
* **Seguridad en smart contracts**: Explotación y mitigación

## **🎓 PROYECTOS REALES Y CERTIFICACIONES**

### **19. Certificaciones**

* **CompTIA Security+**
* **Certified Ethical Hacker (CEH)**
* **Certified Information Systems Security Professional (CISSP)**
* **Certified Information Security Manager (CISM)**

### **20. Proyectos Reales de Ciberseguridad**

* Análisis forense de un ataque a una empresa
* Pentesting en una red local (laboratorio virtual)
* Configuración de un firewall y un IDS/IPS en un entorno simulado
* Realización de un plan de respuesta a incidentes

Este temario cubre **todos los aspectos clave de la ciberseguridad** y te prepara para abordar