ANEXO III

TEMARIO DE LA ESCALA ESPECIAL SUPERIOR DE TECNOLOGIAS DE LA INFORMACIÓN DE LA UNIVERSIDAD AUTÓNOMA DE MADRID

Temario común. Bloque I

1. La Constitución Española de 1978 (I): Estructura. Título Preliminar. Título I: De los derechos y deberes fundamentales. Su garantía y suspensión.
2. La Constitución Española de 1978 (II): Título II: De la Corona. Título III: De las Cortes Generales. Título IX: El Tribunal Constitucional. Título X: La reforma de la Constitución.
3. La Constitución Española de 1978 (III): Título IV: Del Gobierno y de la Administración. Título V: De las relaciones entre el Gobierno y las Cortes Generales. Título VI: Del Poder Judicial. La organización judicial española.
4. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (I): Disposiciones generales. Los interesados en el procedimiento. La actividad de las Administraciones Públicas.
5. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (II): Los actos administrativos: requisitos, eficacia, nulidad y anulabilidad. Disposiciones sobre el procedimiento administrativo común.
6. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (III): Revisión de los actos en vía administrativa. Los recursos administrativos: concepto y clases.
7. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (I): Disposiciones generales, principios de actuación y funcionamiento del sector público.
8. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (II): Organización y funcionamiento del sector público institucional.
9. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (III): Relaciones interadministrativas
10. Ley Orgánica del Sistema Universitario (I): Disposiciones generales, Funciones del sistema universitario y autonomía de las universidades
11. Ley Orgánica del Sistema Universitario (II): Creación y reconocimiento de las universidades y calidad del sistema universitario. Organización de las enseñanzas.
12. Ley Orgánica del Sistema Universitario (II): Cooperación, coordinación y participación en el sistema universitario. El estudiantado en el Sistema Universitario.
13. Estatutos de la Universidad Autónoma de Madrid (I): Naturaleza, funciones, principios rectores y competencias de la UAM. Estructura de la Universidad Autónoma de Madrid. Órganos de Gobierno, representación y administración. Elección y revocación de órganos de gobierno, representación y administración. Defensor del Universitario. La comunidad universitaria.
14. Estatutos de la Universidad Autónoma de Madrid (II): Del estudio y la investigación en la universidad. De la evaluación en la UAM. Servicios universitarios. Régimen económico y financiero. Régimen jurídico y administrativo. Clases y régimen jurídico del personal al servicio de la Universidad Autónoma de Madrid.
15. El Texto Refundido de la Ley del Estatuto Básico del Empleado Público: personal al servicio de las Administraciones Públicas. Derechos y deberes. Adquisición y pérdida de la condición de funcionario. Situaciones administrativas. Régimen disciplinario. Régimen de incompatibilidades. Ingreso en Cuerpos o Escalas de funcionarios. Provisión de puestos de trabajo. Promoción interna.

Bloque II. Temario específico.

16. ENS (RD 311/2022): principios, roles (RSEG/RSI/RS), categorización, medidas de seguridad.
17. RDL 12/2018 y RD 43/2021: seguridad de redes y sistemas; obligaciones para operadores esenciales y proveedores de servicios digitales.
18. Directiva (UE) 2022/2555 – NIS2 y su transposición en España: alcance, gestión de riesgos, reporting, supervisión y régimen sancionador.
19. Estrategia Nacional de Ciberseguridad (2019) y Sistema de Seguridad Nacional: Consejo Nacional de Ciberseguridad, planes y capacidades.
20. RGPD (UE) 2016/679 y LOPDGDD 3/2018: bases jurídicas, DPO, EIPD/DPIA, brechas y sanciones.
21. Reglamento eIDAS y servicios de confianza y el nuevo marco eIDAS2
22. ENI y NTI: documento y expediente electrónico, metadatos, interoperabilidad semántica, técnica y organizativa.
23. Gobierno de TI en AA.PP.: ISO/IEC 38500, COBIT, ITIL v4, políticas, gestión del valor y métricas.
24. Organismos y redes de referencia: CCN/CCNCERT, INCIBE, CERTs/CSIRTs públicos, Red SARA y cooperación europea.
25. MAGERIT v3 y PILAR: identificación de activos, amenazas, estimación y tratamiento del riesgo.
26. ISO/IEC 27001:2022 y 27002:2022: SGSI, Anexo A, control de cambios y auditoría de conformidad.
27. ISO/IEC 27005: gestión del riesgo alineada con ENS y relación con MAGERIT.
28. Continuidad y resiliencia del negocio: ISO 22301 y gestión de BCM/DRP en ciberseguridad.
29. ISO/IEC 27035: gestión de incidentes; preparación, detección, análisis, respuesta y lecciones aprendidas.
30. Auditoría de seguridad: ENS, ISO 19011 y Directrices ISO 27007 y 27008.
31. Guías CCN-STIC relacionadas con ENS, auditoría y bastionado. Perfil de Cumplimiento para universidades.
32. Gobierno del dato y privacidad por diseño: clasificación, minimización, retención y borrado seguro.
33. Gestión de activos TIC y Configuración: Inventario, Ciclo de Vida y CMDB.
34. Métricas, KPIs, KRIs y Reporting en la Gestión de la Seguridad de la Información.
35. Confianza Cero (Zero Trust): principios, ZTNA, SSE, microsegmentación y SASE.
36. Arquitecturas híbridas y multicloud: patrones de referencia (CIS, CSA), control plane y data plane.
37. Seguridad de red corporativa: segmentación L2–L7, SDN y SD-WAN.
38. Alta disponibilidad y resiliencia: clústeres, balanceadores, DRP y pruebas de recuperación.
39. Seguridad física y de instalaciones (CPD): control de accesos, energía, climatización y normativa.
40. MITRE ATT&CK / D3FEND: mapeo de amenazas, controles y detecciones.
41. Modelo de seguridad CIA: Confidencialidad, Integridad y Disponibilidad.
42. Criptografía aplicada: hashing, simétrica/asimétrica, curvas elípticas, gestión de claves post-cuánticas, buenas prácticas y errores comunes.
43. PKI: jerarquías, CP/CPS, OCSP/CRL, automatización ACME y rotación de certificados.
44. Identificación y firma electrónica: DNIe, certificados cualificados, biometría, factores y evidencias.
45. IAM/IdM: ciclo de vida, RBAC/ABAC, mínimo privilegio y segregación de funciones.
46. Autenticación y autorización: Kerberos, RADIUS/TACACS+, SAML, OAuth2, OIDC y FIDO2.
47. Gestión de secretos: bóvedas, KMS/HSM, rotación y control de acceso.
48. Políticas de credenciales: contraseñas, MFA y passkeys.

49. SOC en AA.PP.: misión, modelo operativo, modelo de madurez (SIM3) y acuerdos de nivel de servicio.
50. Detección y telemetría: SIEM y UEBA; correlación de eventos y análisis avanzado.
51. Automatización/SOAR: casos de uso, playbooks, KPIs de eficacia.
52. Gestión de vulnerabilidades: descubrimiento, priorización (CVSS v4), parcheado y verificación.
53. Pentesting y Red Team: PTES/OSSTMM, alcance, legalidad y reglas de enfrentamiento.
54. Threat Hunting y Ciberinteligencia: OSINT, MISP, STIX/TAXII, tipificación de IOCs.
55. Gestión de incidentes: coordinación con CCN-CERT, notificación (ENS/LUCIA) y comunicación de crisis.
56. Forense digital: adquisición (memoria, disco, red), análisis, anti-forense, cadena de custodia e informes.
57. Prevención de fuga (DLP): endpoint, red y nube; metadatos y borrado seguro.
58. Seguridad del puesto: EPP/EDR y XDR, hardening, configuración segura y control de periféricos.
59. Seguridad móvil: MDM/MAM, iOS/Android, contenedores corporativos y BYOD.
60. Seguridad del correo: SPF, DKIM, DMARC, antiphishing, BEC y concienciación.
61. DoS/DDoS: detección, scrubbing, arquitecturas de mitigación y pruebas.
62. Equipos de ciberseguridad: Red Team, Blue Team, Purple Team, White/Gold/Yellow/Green Teams; funciones, métricas y coordinación.
63. Ingeniería social y fraude digital: spear phishing, smishing, vishing, brand abuse y métricas.
64. Programación segura en Python: buenas prácticas, gestión de dependencias, control de errores, librerías seguras y automatización de scripts.
65. Gestión de la interacción con usuarios mediante gestores de incidencias: registro, seguimiento y resolución
66. Firewalls L3/L4 y NGFW: políticas, IDS/IPS, sandboxing e inspección TLS.
67. WAF y protección de aplicaciones: OWASP, bot management y protección de APIs expuestas.
68. DNS seguro: DNSSEC, RPZ, telemetría y uso como sensor de amenazas.
69. Directorios y control de privilegios: LDAP, Active Directory/Entra ID, hardening y PAM.
70. LAN/WAN: VLAN, QoS, SNMP/NetFlow y administración segura.
71. Wi-Fi: IEEE 802.11, WPA3-Enterprise, diseño, autenticación y amenazas.
72. Acceso remoto y VPN: IPsec, SSL VPN, WireGuard y transición hacia ZTNA.
73. VoIP/ToIP (Telefonía IP) y comunicaciones unificadas: SIP/TLS, SRTP y SBC. Amenazas.
74. Almacenamiento y backup: SAN/NAS/objeto, cifrado, inmutabilidad, 3-2-1-1-0 y restauración.
75. Virtualización y VDI: hipervisores, aislamiento, seguridad del plano de gestión.
76. Contenedores y Kubernetes: escaneo de imágenes, políticas (Pod Security), runtime y mTLS.
77. Microservicios y Service Mesh: Istio/Linkerd, políticas, rate limiting y mTLS extremo a extremo.
78. Observabilidad: logs, métricas, trazas, retención y cadena de custodia.
79. IoT e ICS/OT: segmentación, pasarelas, normas sectoriales y particularidades de operación.
80. NDR (Network Detection & Response): sensores, flujos, decodificación y detecciones de movimiento lateral.
81. Seguridad del enrutamiento: BGP, RPKI, Route Origin Validation y MANRS.
82. Correo seguro avanzado: MTA-STS, TLS-RPT, DANE para SMTP TLS, políticas DMARC/BIMI y protección de dominios.
83. Automatización segura de infraestructuras (IaC): Terraform/Ansible, Policy-as-Code (OPA/Conftest).
84. Protocolos de acceso a red: 802.1X, NAC, evaluación de la postura de seguridad.
85. S-SDLC: requisitos de seguridad, modelado de amenazas y revisiones.

86. DevSecOps y CI/CD: pipelines, SAST/DAST/IAST, SBOM, gestión de secretos y artefactos.
87. Seguridad de APIs: autenticación (OAuth2, JWT), control de acceso, rate limiting, validación de datos y protección frente a ataques OWASP API Top 10.
88. Pruebas de aplicaciones web: OWASP ASVS/Top 10, sesiones, CSRF/XSS/SQLi.
89. Seguridad en cloud (IaaS/PaaS/SaaS): IAM, CSPM/CWPP, cifrado, registros y jurisdicción.
90. Evaluación y mejora continua del programa de concienciación en ciberseguridad.
91. Formación y concienciación en ciberseguridad: educación de usuarios y empleados.