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.

Código Seguro De Verificación	444C-3448-6A45P674A-576C	Fecha	28/10/2024
Firmado Por	Ernesto Fernandez Bofill Gonzalez - Gerente - Gerencia		
Url De Verificación	https://sede.uam.es/ValidacionMoviles?codigoFirma=444C-3448-6A45P674A-576C	Página	15/18

Bloque II. Temario específico.

16. La información en las organizaciones. Las organizaciones basadas en la información. La Administración como caso específico de este tipo de organización.
17. Modelos de gobernanza TIC. Organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus organismos públicos. La transformación digital de la Administración General del Estado.
18. Organización y funcionamiento de un centro de sistemas de información. Funciones de desarrollo, mantenimiento, sistemas, bases de datos, comunicaciones, seguridad, calidad, microinformática y atención a usuarios.
19. Planificación y control de las TIC. Gestión de servicios e infraestructuras TIC. Gestión del valor de las TIC. Acuerdos de nivel de servicio. Gestión de incidencias. Objetivos de control y métricas.
20. Gestión IPAM. Protocolo DHCP. Servicio DNS. Securización de DNS mediante DNSSEC.
21. Equipos departamentales y estaciones gráficas de trabajo. Dispositivos personales: PC Portátil, Tablet, Smartphone y otros dispositivos. La conectividad de los dispositivos personales.
22. Dispositivos personales de PC y dispositivos móviles. La conectividad de los dispositivos personales. Medidas de seguridad y gestión para equipos personales y dispositivos móviles.
23. La protección jurídica de los programas de ordenador. Los medios de comprobación de la legalidad y control del software. Tipos de licencias.
24. Gestión de proyectos.
25. Sistemas de almacenamiento para sistemas grandes y departamentales, SAN, NAS, Tecnologías de discos SATA, NL-SAS, SAS y SSD. Tiering. Topologías de almacenamiento de alta disponibilidad.
26. Sistemas operativos Linux. Fundamentos, administración, instalación, gestión.
27. Sistemas operativos Microsoft. Fundamentos, administración, instalación, gestión.
28. Conceptos básicos de otros sistemas operativos: OS X, iOS, Android, z/OS. Sistemas operativos para dispositivos móviles.
29. Seguridad en dispositivos IoT.
30. El cifrado. Algoritmos de cifrado simétricos y asimétricos. La función hash. El notariado.
31. Identificación y firma electrónica. Marco normativo. Prestación de servicios públicos y privados. DNI electrónico, mecanismos biométricos, Smart cards. Gestión de identidades.
32. Infraestructura de clave pública. PKI. Funcionamiento y buenas prácticas. Tipos de certificados según su uso.
33. Adaptación de aplicaciones y entornos a los requisitos de la normativa de protección de datos según los niveles de seguridad. Herramientas de cifrado y auditoría.
34. Sistemas y Tecnologías de Teletrabajo. Herramientas de trabajo en grupo. Sistemas de videoconferencia. Aplicaciones prácticas en la Administración universitaria. Securización en entornos de teletrabajo. La problemática del Shadow IT.
35. Virtualización del puesto de trabajo. Movilidad del puesto de trabajo. Sistemas VDI.
36. Programación en Python.
37. Programación en C++.
38. Aplicaciones web. Lenguaje HTML. CSS. Lenguajes de script. Tecnologías de programación web: CGI, javaScript, applets, servlets, ASP, PHP, JSP. Servidores Web.
39. Web Services: estándares, protocolos asociados. Internacionalización y localización. UTF8. Unicode. Formatos de intercambio de datos (XML, JSON, etc.). Características. Esquemas, conceptos, fundamentos y tipos de datos.
40. Herramientas de gestión de código (VCS). Git. Comunidades de desarrollo colaborativo. Github. Gitlab.
41. Paradigmas de computación distribuida y Servicios en Cloud. IaaS, PaaS, SaaS. Nubes privadas, públicas e híbridas. Securización en entornos en la nube. La seguridad de los servicios cloud públicos. Uso de APIs. CASB.

Código Seguro De Verificación	444C-3448-6A45P674A-576C	Fecha	28/10/2024
Firmado Por	Ernesto Fernandez Bofill Gonzalez - Gerente - Gerencia		
Url De Verificación	https://sede.uam.es/ValidacionMoviles?codigoFirma=444C-3448-6A45P674A-576C	Página	16/18

42. Sistemas de Backup. Políticas de gestión de copias de seguridad. Backup en cloud. Sistemas de recuperación de la información. Seguridad en las copias de seguridad, procedimientos y métodos para la conservación de la información.
43. Proceso de integración continua CI/CD. El pipeline y sus fases. Herramientas.
44. Infraestructura y Sistemas de Documentación Electrónica (InSiDe). Gestión de documentos y expedientes electrónicos ENI.
45. Integración de aplicaciones. Servicios Web SOAP/REST. WSDL. UDDI. Interoperabilidad y seguridad en los servicios Web. WS-S, WS-I.
46. Sistemas de monitorización, gestión y telemetría.
47. Redes Privadas Virtuales. Seguridad en VPN.
48. La red Internet y los servicios básicos.
49. Sistemas de cableado y equipos de interconexión de redes.
50. El modelo de referencia de interconexión de sistemas abiertos (OSI) de ISO: arquitectura, capas, interfaces, protocolos, direccionamiento y encaminamiento.
51. Redes inalámbricas: el estándar IEEE 802.11. Características funcionales y técnicas. Seguridad en redes inalámbricas.
52. Redes IP: arquitectura de redes, encaminamiento y calidad de servicio.
53. Redes de nueva generación y servicios convergentes (NGN/IMS). Seguridad en VoIP, ToIP y comunicaciones unificadas.
54. NAC. 802.1x. Acceso autenticado a redes inalámbrica y cableadas.
55. Redes de área local I. Arquitectura. Tipología. Medios de transmisión. Métodos de acceso. Redes de área extensa.
56. Redes de área local II. Dispositivos de interconexión. Gestión de dispositivos. Administración de redes LAN. Gestión de usuarios en redes locales. Gestión SNMP. Configuración y gestión de redes virtuales (VLAN).
57. Red SARA. Características, securización del acceso y requisitos de acceso por parte de las universidades públicas.
58. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS). Preambulo. Principios básicos. Política de seguridad y principios mínimos de seguridad.
59. Guía CCN-STIC 804: ENS. Guía de implantación.
60. Guías CCN-STIC 881 y 881A: Adecuación al ENS para Universidades. Perfil de cumplimiento específico para Universidades. Política de seguridad para Universidades.
61. Guía CCN-STIC 817: Guía de gestión de ciberincidentes.
62. CCN-CERT, misión y objetivos. Guías Serie 800. Herramientas y soluciones. Instrucciones Técnicas de Seguridad (ITS). Notificación de incidentes de seguridad de conformidad con el ENS.
63. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (LOPDGDD)
64. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 Reglamento General de Protección de Datos (RGPD)
65. Directiva (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022 (NIS2)
66. Estrategia nacional de Ciberseguridad 2019. Consejo nacional de Ciberseguridad.
67. Estándar ISO/IEC 27001:2013 para los Sistemas Gestión de la Seguridad de la Información
68. Sistema de Gestión de la Continuidad de Negocio (ISO22301)
69. ITIL v4
70. Auditoría informática I. Concepto y contenidos. Administración y planificación.
71. Auditoría informática II. Organización, infraestructura técnica y prácticas operativas.
72. Análisis y Gestión de Riesgos. Metodología Magerit v3. Herramientas. Pilar (CCN).
73. Sistemas de Gestión de Seguridad de la Información. Ciclo Deming.

Código Seguro De Verificación	444C-3448-6A45P674A-576C	Fecha	28/10/2024
Firmado Por	Ernesto Fernandez Bofill Gonzalez - Gerente - Gerencia		
Url De Verificación	https://sede.uam.es/ValidacionMoviles?codigoFirma=444C-3448-6A45P674A-576C	Página	17/18

74. Gestión de información y eventos de seguridad (SIEM). Normalización y correlación de eventos. Gestión de alertas. Cuadros de mando.
75. Tecnologías de protección de los equipos e infraestructuras de la empresa, antivirus, antimalware, EDR y XDR.
76. Equipos de ciberseguridad. Equipo rojo. Equipo azul. Equipo violeta.
77. Análisis forense I. Equipo de trabajo mínimo. Clonación de información. Adquisición de evidencias. Cadena de custodia.
78. Análisis forense II. Fases. Análisis en distintos SO. Herramientas. Peritaje. Informes técnico y ejecutivo.
79. Fases, desarrollo y tipos de los ataques informáticos.
80. Bastionado de Linux.
81. Bastionado de Windows.
82. Automatización I. Metodologías y tecnologías. Arquitectura como código. Devops.
83. Automatización II. Orquestación de seguridad. Devsecops. Herramientas.
84. Detección y protección de ataques en red en tiempo real. IDS/IPS
85. Despliegue de aplicaciones como microservicios. Contenedores. Docker. Kubernetes.
86. Gestión de ciberinteligencia. Tipos de IoCs. Técnicas de recopilación y gestión. Validez y tiempo de vida.
87. La seguridad en redes. Seguridad perimetral. Herramientas de seguridad contra ataques: cortafuegos de nivel 3 y 4, cortafuegos de nueva generación, control de accesos e intrusiones, técnicas criptográficas, etc.
88. Ataques de Denegación de servicio. (DoS y DDoS) técnicas de ataque y contramedidas de protección.
89. El correo electrónico. Funcionamiento, configuraciones y protocolos de seguridad SPF, DKIM, DMARC.
90. IPv6. Transición y convivencia IPv4-IPv6. Métodos de despliegue. Características.

Código Seguro De Verificación	444C-3448-6A45P674A-576C	Fecha	28/10/2024
Firmado Por	Ernesto Fernandez Bofill Gonzalez - Gerente - Gerencia		
Url De Verificación	https://sede.uam.es/ValidacionMoviles?codigoFirma=444C-3448-6A45P674A-576C	Página	18/18