

TEMARIO FORMATIVO ISMS FORUM

Curso Gobierno de Ciberseguridad en la Nube

El curso es preparador de la certificación
profesional CCGP -Certified Cloud
Cybersecurity Governance Professional

isms
FORUM



DOMINIO	SUBDOMINIOS
1. Conceptos básicos de la Nube	<p>1.1 Introducción y Definiciones:</p> <ul style="list-style-type: none"> a) El paradigma de la Nube: Definición, Historia y base tecnológica de la Nube. b) Nube vs tecnologías de Nube vs Servicios en la Nube; Nube vs OnPrem; CSP vs CU/CSC; Publica vs Privada; IaaS vs PaaS vs SaaS; Concepto de Tenancy. c) Identificación de Ejemplos y taxonomía de Servicios en la Nube d) Entornos híbridos y multicloud e) Arquitecturas cloud <p>1.2 Servicios Avanzados en la Nube:</p> <ul style="list-style-type: none"> a) Ejemplos de casos de uso especializados en Nube: DRaaS, SECaaS, IDaaS, BPaaS, ... b) Catálogo de soluciones disponibles c) Infoestructura vs. Applistructure vs. Metaestructura vs. Infraestructura d) Roles y responsabilidades en la Nube: Competencias y cualidades específicas de las personas para trabajo en la Nube
2. Cloud-Economics & FinOps	<p>2.1 ¿Por qué la Nube no es solo tecnología?</p> <p>2.2. Impacto de la Nube en el Negocio Actual: economías, automatización, eficiencias</p> <p>2.3 Taxonomía de Modelos de Negocio asociados, desarrollados o soportados en la Nube.</p> <p>2.4 Análisis detallado de Modelos de Negocio en Nube más extendidos</p> <ul style="list-style-type: none"> a) Servicios verticales sobre PaaS/IaaS pública b) Web Service OnPrem vs Cloud SaaS c) Otros modelos <p>2.4 FinOps</p> <p>2.5 Shared responsibility model</p>
3.GRC de la Nube	<p>3.1. Modelos gobierno específicos Cloud</p> <ul style="list-style-type: none"> c) Modelos Generales de Gobierno de Nube: CCoE y CAC. Cloud Security Champions <p>3.2 Riesgos en y de la Nube</p> <ul style="list-style-type: none"> a) Metodologías de Análisis de Riesgos para la Nube b) Amenazas Específicas para Entorno y Servicios en la Nube: CSA Top-Threats c) Nuevos Riesgos Propios de la Nube <p>3.3 Marcos de control Cloud</p> <ul style="list-style-type: none"> a) Guía CSA de controles para la Nube b) La CCM, Cloud Control Matrix, como herramienta operativa c) El Cuestionario de Autoevaluación CAIQ d) Certificación CSA-STAR e) CSA y EU Cloud Code of Conduct (EU Cloud CoC) f) Otras herramientas CSA. <p>3.4 Cumplimiento en y de la Nube</p> <ul style="list-style-type: none"> a) La Nube, Cumplimiento Legal y Soberanía Digital. b) Aplicación a la Nube de Regulaciones: Privacidad (GDPR y LOPD-GDD), Regulaciones UE (DORA, NIS y NIS2, Reglamento Inteligencia Artificial) y Nacionales (ENS). <p>3.5 Crime prosecution en entorno Cloud</p> <p>3.6 Marcos de control internacionales: NIST, CSF, ISO 27017, C5, Cobit, CISA.</p>

4. Controles

4.1 Gestión de identidades en la Nube.

- a) Gestión de identidades en la Nube. Cloud IAM + CIEM.
- b) Modelos de identidad digital: centralizada, descentralizada, federación ..
- c) Servicios IDaaS (Identity as a service). Brokering de Identidades
- d) Mejores prácticas en la gestión de identidades en la nube
- e) Tendencias y desafíos futuros

4.2 Cifrado en la Nube

- a) Casos de uso: Cifrado at Rest, on Transit & on Process (y cifrado homomórfico)
- b) Gestión de Claves en la Nube: PKMS, KMSaaS, HSMaaS y otras. Casos de Uso.
- c) Estrategias de Implantación de Cifrado en la Nube.
- d) Arquitecturas de cifrado y casos de uso.
- e) Tecnologías y tecnologías emergentes.

4.3 Gestión de vulnerabilidades y parcheo de servicios en la Nube vs. OnPrem

- a) Prevención y resiliencia en la Nube
- b) Gestión de vulnerabilidades en la Nube. De VM a TVM. Herramientas y tecnologías.
- c) Parcheo en la nube Vs OnPremise
- d) CSPM (Cloud Security Posture Management)

4.3 Gestión de vulnerabilidades y parcheo de servicios en la Nube vs. OnPrem

- e) Seguridad en contenedores y MVs
- f) Aplantillado de servicios y plataformas.
- g) Gestión de la Configuración en la Nube: MaaS y Automatización.
- h) CWPP (Cloud Workload Protection Platforms)
- i) CNAPP (Cloud-Native Application Protection Platforms)

4.4 Seguridad de Red en la Nube.

- a) La Nube y SDNs (Software-Defined Networks). Taxonomía
- b) SDWANs. Aplicación para Arquitecturas de Nube.
- c) Microsegmentación. Aplicación a los servicios en Nube. Relación con SDN y SDWAN.
- b) Gestión de movilidad y acceso ubicuo a workloads
- c) SASE, ZeroTrust y SWG

4.5 Nube híbrida y MultiCloud

- a) Integración de servicios Cloud en TI corporativa
- b) Integración de monitorización Cloud en TI corporativa
- c) Entornos Multicloud y su gestión: ventajas e inconvenientes

4.6 Gestión del Pentesting en la Nube

- a) Pentesting en la Nube. Consideraciones Particulares.
- b) Análisis Forense en la Nube. Consideraciones Particulares.
- c) Auditoría de Seguridad en la Nube. Concepto de Auditoría Continua.

- 4.7 Respuesta ante incidentes en la Nube
 - a) Marcos de referencia: NIST, STIC, PICERL, 27xxx
 - b) Incident Responde vs. Cloud Incident Response
 - c) Roles de usuarios y proveedores. Influencia del Modelo de Responsabilidad Compartida
 - d) Modelado de playbooks en Cloud
 - e) Ejecución en Cloud de fases de respuesta.

4.8 Edge computing, serverless, mobile computing and remote working.

- a) Consideraciones de Arquitectura serverless
- b) definición y aplicación de Edge computing.
- c) Evolución hacia modelos de Servicios avanzados.

4.9 Servicios basados en Datos: IA, ML; BigData. Data Governance en la Nube.

4.10 Cloud SecDevOps

- a) DevOps y metodologías ágiles. OWASP
- b) Security by default & by design en el desarrollo y adopción de servicios cloud
- c) Entornos en cloud para Integración Continua (CI) y Entrega Continua (CD)
- d) Perfiles, roles y responsabilidades
- e) Threat Modelling. Metodología Stride.
- f) SSDLC aplicado a Cloud
- g). Ejemplo práctico de CI/CD con Jenkins

4.11 IOT on Cloud. Infraestructuras Críticas y Servicios Esenciales

- a) Evolución TI vs TI/OT/XIoT
- b) Amenazas y Regulaciones
- c) Uso de XIoT en Infraestructuras Críticas: Restos, Riesgos y Recomendaciones
- d) Arquitecturas de Seguridad OT
- e) Servicios de Ciberseguridad OT en el mercado

5. Gestión contractual

5.1 Adquisición de Servicios de la Nube

- a) Proceso de adquisición de servicios. No todas las Nubes se contratan igual.
- b) Modelos de contratación disponibles: compra, suscripción, licenciamiento y otros.
- c) Condiciones exigibles, deseables y óptimas para el Usuario de la Nube.
- d) Negociación con el proveedor: Necesidad, Capacidad
- e) Casos prácticos de escenarios de adquisición de servicios de la Nube.

5.2 Clausulado contractual para Servicios de la Nube

- a) Proceso de Creación de Contrato para Servicios en la Nube
- b) Documentación contractual vs documentación NoContractual/Informativa. Disponibilidad, diferencias y grado de exigibilidad.
- c) Documentación deseable vs documentación mínima.
- d) Contenidos y clausulado del contrato de interés para el Usuario de la Nube: resultados de DueDiligence, SLA, cláusulas tipo de privacidad, Plan de Salida, otros requisitos contractuales.
- e) Particularidades Sectoriales: Banca, Sector Público, otros. Reguladores. Requisitos y expectativas sectoriales.
- f) Riesgos derivados de marco contractual deficitario / incompleto / no viable
- g) Transferencias de riesgos contractuales

5.3 Gestión de Proveedores de la Nube

a) Gestión de Servicios vs Gestión de Proveedores

a) Herramientas de seguimiento disponibles: propiedad, tipología y aplicabilidad.

c) Seguimiento y Cumplimiento de SLAs. Parámetros habituales y sus valores.

d) Integración y Orquestación de Gobierno y Gestión TI con proveedores de la Nube: reporte, controles, herramientas.

6.1 Evolución de las organizaciones por la adopción de servicios en la Nube

a) Impacto de la Nube: Diferencias entre Outsourcing y CSP

6. Impacto en la organización

b) Impacto de la Nube en Procesos de la Organización: Distribución, automatización, reingeniería

c) Impacto de la Nube en estrategia, presupuestos y organización.

d) Impacto de la Nube en personas: evolución de roles y perfiles de TI, de Seguridad y otros. Impacto

e) Impacto de la Nube en las tecnologías

Simulacro examen



INTERNATIONAL
INFORMATION
SECURITY
COMMUNITY