Referencial de competencias profesionales

Formación Cloud Computing y Arquitectura Cloud

País: Spain

Profesiones cubiertas: Cloud Computing y Arquitectura Cloud

Este referencial es una certificación profesional privada, inspirada en los estándares de los referenciales de certificación franceses (metodología France Compétences). No constituye un referencial estatal.

Generado el 09/06/2026

Índice

ANEXO I Presentación sintética del marco del diploma

PRESENTACIÓN GENERAL

Nombre de la formación: Certificado de Profesionalidad en Cloud Computing y Arquitectura Cloud

Tipo de certificación: Certificado de Profesionalidad

Modalidades de formación:

Formación presencial, semipresencial y a distancia con prácticas en entornos cloud reales (AWS, Azure, GCP)

Finalidad y objetivos:

Capacitar profesionales para diseñar, provisionar, automatizar y operar infraestructuras cloud escalables y seguras. Los participantes desarrollarán competencias en arquitectura cloud, Infrastructure as Code, seguridad, monitoreo, migración de aplicaciones y optimización de costes. Al finalizar, serán capaces de diseñar soluciones cloud alineadas con objetivos empresariales, implementar controles de seguridad, automatizar operaciones mediante IaC, monitorear rendimiento de servicios, gestionar continuidad de negocio y liderar transformación organizativa hacia cloud.

Contexto profesional:

El Cloud Computing y la Arquitectura Cloud son disciplinas críticas en la transformación digital de organizaciones. Los profesionales en este campo diseñan y operan infraestructuras cloud que soportan aplicaciones empresariales críticas. Trabajan en entornos altamente dinámicos, colaborando con equipos de desarrollo, operaciones y negocio. Requieren conocimiento profundo de proveedores cloud públicos (AWS, Azure, GCP), patrones arquitectónicos modernos, herramientas de automatización y prácticas de seguridad. La demanda de estos profesionales es muy alta en España, con oportunidades en empresas de todos los sectores que adoptan cloud.

Público objetivo y condiciones de acceso:

Profesionales con experiencia en infraestructura IT, administración de sistemas, desarrollo de software o arquitectura de sistemas que deseen especializarse en cloud computing. También dirigido a profesionales en transición que busquen adquirir competencias cloud para mejorar su empleabilidad.

Prerrequisitos:

- Conocimientos básicos de redes (TCP/IP, DNS, firewalls)
- Experiencia en administración de sistemas operativos (Linux/Windows)
- Familiaridad con línea de comandos y scripting básico
- Comprensión de conceptos de virtualización
- Inglés técnico a nivel intermedio para documentación y herramientas

Vías de acceso:

- formation_continue
- enseignement_a_distance

ORGANIZACIÓN DE LA FORMACIÓN

Enfoque pedagógico:

La formación combina teoría fundamentada en marcos de referencia reconocidos (AWS Well-Architected, Azure Architecture) con práctica intensiva en entornos cloud reales. Se utiliza metodología de aprendizaje basado en proyectos, donde los participantes diseñan e implementan soluciones cloud completas.

- Aprendizaje basado en proyectos con casos de uso reales de migración y modernización
- Laboratorios prácticos en entornos cloud públicos (AWS, Azure, GCP) con acceso a cuentas de prueba
- Análisis de decisiones arquitectónicas (ADRs) documentadas en proyectos reales
- Simulacros de incidentes y recuperación ante desastres para desarrollar capacidad de respuesta
- Revisión de código IaC y configuraciones de seguridad con retroalimentación especializada
- Mentoría de profesionales con experiencia en transformación cloud empresarial
- Evaluación continua mediante pruebas prácticas de diseño, implementación y operación

Métodos de aprendizaje:

- Clases magistrales con demostraciones en vivo de herramientas cloud
- Laboratorios prácticos guiados en entornos cloud
- Proyectos de equipo con entregables documentados
- Análisis de casos de estudio de migraciones y modernizaciones reales
- Sesiones de resolución de problemas y troubleshooting
- Webinars con expertos de proveedores cloud
- Estudio independiente de documentación técnica y mejores prácticas

Puntos fuertes de la formación:

- Cobertura exhaustiva de 12 áreas funcionales de cloud computing desde diseño hasta optimización
- Enfoque práctico con laboratorios en múltiples proveedores cloud (AWS, Azure, GCP)
- Énfasis en seguridad y cumplimiento normativo integrado en todas las unidades
- Desarrollo de competencias de liderazgo y transformación organizativa
- Alineación con marcos de referencia reconocidos internacionalmente
- Preparación para certificaciones profesionales de proveedores cloud
- Acceso a herramientas y plataformas cloud reales durante la formación
- Formadores con experiencia práctica en proyectos cloud empresariales

TABLA DE SÍNTESIS DE ACTIVIDADES - BLOQUES DE COMPETENCIAS - UNIDADES

Actividades	Bloques de competencias	Unidades
Función 1: Diseño y Evaluación de Arquitecturas Cloud • Diseñar arquitecturas cloud escalables y resilientes • Evaluar proveedores y servicios cloud • Seleccionar modelos de servicio cloud (IaaS, PaaS, SaaS, FaaS) • Seleccionar modelos de despliegue cloud (público, privado, híbrido, multi-cloud)	**Bloque 1 - Diseño y Evaluación de Arquitecturas Cloud** • Diseñar arquitecturas cloud híbridas estableciendo conectividad segura entre entornos on-premises y cloud para mantener flexibilidad operativa	**Unidad U1 Diseño y Evaluación de Arquitecturas Cloud**
Función 2: Provisión y Configuración de Infraestructura Cloud • Provisionar servicios en plataformas cloud públicas • Desplegar infraestructuras cloud privadas • Configurar entornos cloud híbridos • Diseñar soluciones de red en entornos cloud	**Bloque 2 - Provisión y Configuración de Infraestructura Cloud** • Provisionar servicios cloud públicos mediante herramientas de Infrastructure as Code garantizando reproducibilidad, versionado y trazabilidad de configuraciones	**Unidad U2 Provisión y Configuración de Infraestructura Cloud**
Función 3: Automatización e Infraestructura como Código • Desarrollar scripts y pipelines de automatización de infraestructura • Implementar herramientas de Infrastructure as Code (IaC) • Gestionar configuración y detectar desviaciones (configuration drift)	**Bloque 3 - Automatización e Infraestructura como Código**	**Unidad U3 Automatización e Infraestructura como Código**
Función 4: Operación y Monitoreo de Servicios Cloud • Configurar herramientas de monitoreo y observabilidad • Definir SLIs, SLOs y analizar tendencias de rendimiento • Gestionar incidentes y resolver problemas operativos • Operar servicios empresariales en la nube	**Bloque 4 - Operación, Monitoreo y Optimización de Servicios Cloud**	**Unidad U4 Operación, Monitoreo y Optimización de Servicios Cloud**
Función 5: Gestión de Servidores, Software y Contenedores • Administrar instancias de cómputo cloud • Gestionar el ciclo de vida de aplicaciones y servicios software • Administrar plataformas de orquestación de contenedores	**Bloque 5 - Gestión de Servidores, Software y Contenedores** • Administrar ciclo de vida de instancias cloud aplicando hardening y configuración segura para garantizar disponibilidad y seguridad operativa • Orquestar contenedores en plataformas cloud utilizando Kubernetes para automatizar despliegue, escalado y gestión del ciclo de vida de aplicaciones	**Unidad U5 Gestión de Servidores, Software y Contenedores**

Actividades	Bloques de competencias	Unidades
Función 6: Integración de Sistemas y Arquitecturas de Mensajería • Integrar servicios cloud con sistemas existentes • Implementar soluciones de mensajería y eventos en cloud	**Bloque 6 - Integración de Sistemas y Arquitecturas de Mensajería** • Integrar soluciones cloud con sistemas heredados mediante APIs, colas de mensajes y buses de eventos para garantizar interoperabilidad y consistencia de datos • Implementar soluciones de mensajería y eventos en cloud diseñando arquitecturas asíncronas para desacoplamiento de componentes y escalabilidad	**Unidad U6 Integración de Sistemas y Arquitecturas de Mensajería**
Función 7: Seguridad Cloud y Cumplimiento Normativo • Aplicar buenas prácticas de desarrollo seguro en cloud • Definir e implementar controles de seguridad cloud • Administrar identidades y accesos en la nube • Identificar y mitigar vulnerabilidades de seguridad • Asegurar cumplimiento normativo y promover cultura de seguridad	**Bloque 7 - Seguridad Cloud y Cumplimiento Normativo** • Configurar controles de seguridad en entornos cloud aplicando modelo de responsabilidad compartida para proteger datos y servicios contra amenazas • Aplicar prácticas de desarrollo seguro integrando análisis de vulnerabilidades en pipelines DevOps para identificar y mitigar riesgos de seguridad tempranamente • Administrar identidades y accesos en cloud aplicando principio de mínimo privilegio para controlar autorización y auditar acceso a recursos	**Unidad U7 Seguridad Cloud y Cumplimiento Normativo**
Función 8: Almacenamiento, Datos y Bases de Datos Cloud • Diseñar soluciones de almacenamiento cloud • Administrar bases de datos en la nube • Migrar datos a la nube	**Bloque 8 - Almacenamiento, Datos y Bases de Datos Cloud** • Diseñar arquitecturas cloud escalables y resilientes aplicando patrones arquitectónicos modernos para satisfacer requisitos de disponibilidad y rendimiento • Migrar datos a cloud garantizando integridad, seguridad y validación mediante procesos automatizados y reconciliación de datos	**Unidad U8 Almacenamiento, Datos y Bases de Datos Cloud**
Función 9: Continuidad, Recuperación y Copias de Seguridad • Diseñar planes de continuidad y recuperación ante desastres • Implementar políticas y procedimientos de backup • Restaurar servicios tras incidentes cloud	**Bloque 9 - Continuidad, Recuperación y Copias de Seguridad** • Diseñar e implementar planes de continuidad de negocio y recuperación ante desastres definiendo RTO y RPO para garantizar resiliencia operativa	**Unidad U9 Continuidad, Recuperación y Copias de Seguridad**
Función 10: Migración de Aplicaciones y Adopción Cloud • Planificar y ejecutar migraciones de aplicaciones • Definir estrategias de adopción cloud • Gestionar cambios organizativos y capacitación en adopción cloud	**Bloque 10 - Migración de Aplicaciones y Adopción Cloud** • Monitorear rendimiento de servicios cloud mediante métricas, trazas distribuidas y análisis de tendencias para garantizar cumplimiento de SLOs • Planificar y ejecutar migraciones de aplicaciones a cloud seleccionando estrategias (rehost, replatform, refactor) según requisitos técnicos y empresariales	**Unidad U10 Migración de Aplicaciones y Adopción Cloud**

Actividades	Bloques de competencias	Unidades
Función 11: Optimización de Costes y Recursos Cloud • Analizar uso de recursos y optimizar infraestructura cloud • Gestionar costes y presupuestos cloud	**Bloque 11 - Optimización de Costes y Recursos Cloud** • Evaluar y seleccionar proveedores cloud públicos considerando capacidades técnicas, cumplimiento normativo y análisis económico para alinearse con estrategia empresarial • Optimizar infraestructura cloud mediante rightsizing, gestión de instancias reservadas y análisis de costes para maximizar eficiencia económica	**Unidad U11 Optimización de Costes y Recursos Cloud**
Función 12: Gestión de Proyectos, Documentación y Comunicación Cloud • Coordinar y seguimiento de proyectos cloud • Documentar configuraciones y decisiones de arquitectura cloud • Comunicar estado operativo y facilitar colaboración en iniciativas cloud	**Bloque 12 - Gestión de Proyectos, Documentación y Comunicación Cloud** • Documentar arquitecturas cloud mediante decisiones arquitectónicas (ADRs) y runbooks operativos para facilitar mantenimiento y transferencia de conocimiento • Coordinar proyectos de adopción cloud gestionando cronograma, recursos y riesgos para asegurar entrega exitosa y alineación con objetivos empresariales • Liderar transformación organizativa hacia cloud promoviendo cambio cultural, capacitación y adopción de nuevas prácticas entre equipos • Alinear soluciones cloud con objetivos empresariales traduciendo requisitos de negocio a especificaciones técnicas para garantizar valor agregado	**Unidad U12 Gestión de Proyectos, Documentación y Comunicación Cloud**

Tabla de síntesis de funciones y actividades

Función 1: Diseño y Evaluación de Arquitecturas Cloud
Actividad 1.1 Diseñar arquitecturas cloud escalables y resilientes
Actividad 1.2 Evaluar proveedores y servicios cloud
Actividad 1.3 Seleccionar modelos de servicio cloud (IaaS, PaaS, SaaS, FaaS)
Actividad 1.4 Seleccionar modelos de despliegue cloud (público, privado, híbrido, multi-cloud)
Función 2: Provisión y Configuración de Infraestructura Cloud
Actividad 2.1 Provisionar servicios en plataformas cloud públicas
Actividad 2.2 Desplegar infraestructuras cloud privadas
Actividad 2.3 Configurar entornos cloud híbridos
Actividad 2.4 Diseñar soluciones de red en entornos cloud
Función 3: Automatización e Infraestructura como Código
Actividad 3.1 Desarrollar scripts y pipelines de automatización de infraestructura
Actividad 3.2 Implementar herramientas de Infrastructure as Code (IaC)
Actividad 3.3 Gestionar configuración y detectar desviaciones (configuration drift)
Función 4: Operación y Monitoreo de Servicios Cloud
Actividad 4.1 Configurar herramientas de monitoreo y observabilidad
Actividad 4.2 Definir SLIs, SLOs y analizar tendencias de rendimiento
Actividad 4.3 Gestionar incidentes y resolver problemas operativos
Actividad 4.4 Operar servicios empresariales en la nube
Función 5: Gestión de Servidores, Software y Contenedores
Actividad 5.1 Administrar instancias de cómputo cloud
Actividad 5.2 Gestionar el ciclo de vida de aplicaciones y servicios software
Actividad 5.3 Administrar plataformas de orquestación de contenedores
Función 6: Integración de Sistemas y Arquitecturas de Mensajería
Actividad 6.1 Integrar servicios cloud con sistemas existentes
Actividad 6.2 Implementar soluciones de mensajería y eventos en cloud
Función 7: Seguridad Cloud y Cumplimiento Normativo
Actividad 7.1 Aplicar buenas prácticas de desarrollo seguro en cloud
Actividad 7.2 Definir e implementar controles de seguridad cloud
Actividad 7.3 Administrar identidades y accesos en la nube
Actividad 7.4 Identificar y mitigar vulnerabilidades de seguridad
Actividad 7.5 Asegurar cumplimiento normativo y promover cultura de seguridad
Función 8: Almacenamiento, Datos y Bases de Datos Cloud

Actividad 8.1 Diseñar soluciones de almacenamiento cloud
Actividad 8.2 Administrar bases de datos en la nube
Actividad 8.3 Migrar datos a la nube
Función 9: Continuidad, Recuperación y Copias de Seguridad
Actividad 9.1 Diseñar planes de continuidad y recuperación ante desastres
Actividad 9.2 Implementar políticas y procedimientos de backup
Actividad 9.3 Restaurar servicios tras incidentes cloud
Función 10: Migración de Aplicaciones y Adopción Cloud
Actividad 10.1 Planificar y ejecutar migraciones de aplicaciones
Actividad 10.2 Definir estrategias de adopción cloud
Actividad 10.3 Gestionar cambios organizativos y capacitación en adopción cloud
Función 11: Optimización de Costes y Recursos Cloud
Actividad 11.1 Analizar uso de recursos y optimizar infraestructura cloud
Actividad 11.2 Gestionar costes y presupuestos cloud
Función 12: Gestión de Proyectos, Documentación y Comunicación Cloud
Actividad 12.1 Coordinar y seguimiento de proyectos cloud
Actividad 12.2 Documentar configuraciones y decisiones de arquitectura cloud
Actividad 12.3 Comunicar estado operativo y facilitar colaboración en iniciativas cloud

Estas áreas, desglosadas en actividades que el profesional realiza con autonomía o bajo supervisión, pueden no ejercerse todas en la entidad empleadora, especialmente en un primer empleo.

ANEXO II Marco de actividades profesionales

Contexto profesional y empleos

El Cloud Computing y la Arquitectura Cloud constituyen disciplinas fundamentales en la transformación digital contemporánea. Los profesionales en este campo diseñan, implementan y operan infraestructuras cloud que soportan aplicaciones empresariales críticas. Trabajan en la intersección entre tecnología y estrategia empresarial, traduciendo requisitos de negocio en soluciones técnicas escalables, seguras y económicamente eficientes. El rol requiere dominio profundo de proveedores cloud públicos (AWS, Azure, Google Cloud Platform), patrones arquitectónicos modernos (microservicios, serverless, contenedores), herramientas de automatización (Terraform, Kubernetes, Ansible) y prácticas de seguridad integradas (DevSecOps). Los profesionales colaboran constantemente con equipos de desarrollo, operaciones, seguridad y negocio, requiriendo habilidades de comunicación técnica y liderazgo. La demanda de estos profesionales en España es muy elevada, con oportunidades en empresas de todos los sectores que adoptan o modernizaban infraestructuras cloud.

La persona titulada desempeña diferentes funciones:
– diseño y evaluación de arquitecturas cloud ;
– provisión y configuración de infraestructura cloud ;
– automatización e infraestructura como código ;
– operación y monitoreo de servicios cloud ;
– gestión de servidores, software y contenedores ;
– integración de sistemas y arquitecturas de mensajería ;
– seguridad cloud y cumplimiento normativo ;
– almacenamiento, datos y bases de datos cloud ;
– continuidad, recuperación y copias de seguridad ;
– migración de aplicaciones y adopción cloud ;
– optimización de costes y recursos cloud ;
– gestión de proyectos, documentación y comunicación cloud ;

Empleos relacionados

Los empleos de estos profesionales se encuentran en distintas estructuras públicas y privadas, entre ellas:
– Grandes empresas con transformación digital en curso ;
– Empresas de servicios cloud y consultoría tecnológica ;
– Proveedores de servicios gestionados (MSP) con oferta cloud ;
– Departamentos de IT corporativos en sectores financiero, sanitario, retail y manufactura ;
– Startups y empresas de tecnología con infraestructura cloud nativa ;
– Organismos públicos modernizando infraestructura IT ;
– Empresas de integración de sistemas y transformación digital ;

Los puestos reciben denominaciones diferentes según el sector. Algunos ejemplos son:
– Arquitecto Cloud ;
– Ingeniero Cloud ;
– Especialista en Cloud Computing ;
– Administrador de Infraestructura Cloud ;
– Ingeniero DevOps Cloud ;
– Especialista en Seguridad Cloud ;

– Consultor de Arquitectura Cloud ;
– Gestor de Operaciones Cloud ;
– Especialista en Migración Cloud ;
– Ingeniero de Automatización Cloud ;

Compensación de Entrada en el Mercado Laboral Español

Los profesionales con Certificado de Profesionalidad en Cloud Computing y Arquitectura Cloud pueden esperar salarios iniciales entre 28.000 y 35.000 euros anuales, dependiendo de experiencia previa, ubicación geográfica y sector. En Madrid y Barcelona, los salarios tienden a ser 10-15% superiores. Con experiencia de 2-3 años, los salarios pueden alcanzar 40.000-50.000 euros. Especialistas senior con 5+ años de experiencia pueden superar 60.000 euros. Factores como certificaciones de proveedores cloud (AWS Solutions Architect, Azure Administrator), experiencia en seguridad cloud y liderazgo de proyectos incrementan significativamente la compensación.

Evolución profesional (3 a 5 años)

Los profesionales en Cloud Computing y Arquitectura Cloud tienen trayectorias de carrera diversas y ascendentes. Pueden especializarse en áreas específicas o evolucionar hacia roles de liderazgo y estrategia.

- Arquitecto Cloud Senior: Liderazgo técnico en diseño de soluciones cloud empresariales complejas
- Gestor de Transformación Cloud: Coordinación de iniciativas de adopción cloud a nivel organizativo
- Especialista en Seguridad Cloud: Enfoque profundo en seguridad, cumplimiento y gobernanza cloud
- Consultor de Arquitectura Cloud: Asesoramiento a múltiples clientes en diseño de soluciones cloud
- Gestor de Operaciones Cloud: Responsabilidad de operación y optimización de infraestructura cloud
- Especialista en Migración Cloud: Liderazgo de proyectos complejos de migración de aplicaciones
- Ingeniero de Plataforma Cloud: Desarrollo de plataformas cloud internas para equipos de desarrollo
- Director de Infraestructura Cloud: Liderazgo estratégico de infraestructura cloud empresarial

Continuación de estudios

Los profesionales pueden continuar su desarrollo mediante: (1) Certificaciones profesionales de proveedores cloud (AWS Solutions Architect Professional, Azure Solutions Architect Expert, Google Cloud Architect); (2) Especializaciones en seguridad cloud (CCSK - Certified Cloud Security Knowledge); (3) Formación en gobernanza y cumplimiento normativo (ISO 27001, SOC 2); (4) Estudios superiores en Ingeniería de Sistemas o Máster en Cloud Computing; (5) Certificaciones en gestión de proyectos (PMP, PRINCE2) para evolucionar hacia roles de liderazgo.

ÉTICA Y DEONTOLOGÍA PROFESIONAL

La práctica profesional en Cloud Computing y Arquitectura Cloud requiere compromiso con principios éticos fundamentales que garanticen seguridad, privacidad y responsabilidad.

- Responsabilidad en seguridad: Aplicar consistentemente estándares de seguridad y proteger datos contra amenazas, priorizando seguridad sobre conveniencia operativa
- Privacidad y cumplimiento normativo: Respetar derechos de privacidad de usuarios y cumplir regulaciones (GDPR, LSSI-CE) en tratamiento de datos
- Transparencia en decisiones técnicas: Documentar decisiones arquitectónicas claramente, explicar trade-offs y justificar recomendaciones a stakeholders
- Integridad en evaluación de soluciones: Evaluar alternativas de forma objetiva, documentar criterios de evaluación y evitar sesgos hacia proveedores específicos

• Responsabilidad operativa: Monitorear sistemas proactivamente, responder rápidamente a incidentes y mantener disponibilidad de servicios críticos
• Sostenibilidad ambiental: Optimizar consumo de recursos cloud, considerar impacto ambiental de decisiones de infraestructura
• Equidad en acceso: Garantizar que soluciones cloud sean accesibles a usuarios con diferentes capacidades y contextos tecnológicos
• Honestidad en limitaciones: Reconocer limitaciones técnicas de soluciones, comunicar riesgos claramente y evitar promesas no realistas

Función 1: Diseño y Evaluación de Arquitecturas Cloud

Función 1: Diseño y Evaluación de Arquitecturas Cloud

Actividad 1.1 Diseñar arquitecturas cloud escalables y resilientes

- Definir la estructura técnica de soluciones cloud capaces de escalar horizontal y verticalmente según la demanda
  - ■ Seleccionar patrones arquitectónicos adecuados (microservicios, serverless, contenedores) en función de los requisitos de negocio
  - ■ Documentar los diagramas de referencia de la arquitectura incluyendo componentes, relaciones y flujos de datos
  - ■ Garantizar que la arquitectura cumpla con los requisitos de escalabilidad, disponibilidad y rendimiento
- Aplicar principios de diseño de arquitecturas flexibles y resilientes
  - ■ Incorporar principios de loose coupling, alta cohesión y resiliencia en el diseño
  - ■ Aplicar marcos de referencia como AWS Well-Architected Framework o Azure Architecture Framework
  - ■ Diseñar mecanismos de recuperación ante fallos y redundancia
- Revisar periódicamente la arquitectura y proponer mejoras
  - ■ Realizar revisiones arquitectónicas periódicas para identificar oportunidades de mejora
  - ■ Evaluar la alineación de la arquitectura con los objetivos empresariales actuales
  - ■ Documentar las decisiones arquitectónicas (ADRs) y su justificación

■ Medios y recursos

- Herramientas de modelado de arquitectura (Lucidchart, Draw.io, ArchiMate)
- Marcos de referencia (AWS Well-Architected Framework, Azure Architecture Framework, TOGAF)
- Documentación de patrones arquitectónicos (microservicios, serverless, contenedores)
- Repositorios de decisiones arquitectónicas (ADR templates)

■ Resultados esperados

- Diagramas de arquitectura documentados y validados
- Decisiones arquitectónicas justificadas y registradas
- Arquitectura que cumple con requisitos de escalabilidad, disponibilidad y rendimiento
- Plan de mejora continua de la arquitectura

Función 1: Diseño y Evaluación de Arquitecturas Cloud

Actividad 1.2 Evaluar proveedores y servicios cloud

- Analizar y comparar proveedores cloud (AWS, Azure, GCP) en función de criterios técnicos, económicos y de cumplimiento normativo
  - ■ Elaborar matrices de evaluación que incluyan criterios de rendimiento, seguridad, cumplimiento y coste
  - ■ Recopilar información sobre capacidades técnicas, SLAs y opciones de soporte de cada proveedor
  - ■ Validar la idoneidad de cada solución frente a los requisitos del negocio
- Elaborar recomendaciones documentadas sobre la selección de proveedores
  - ■ Presentar análisis comparativos a los responsables de decisión
  - ■ Justificar la recomendación en función de los criterios de evaluación

    - ■ Documentar los riesgos y limitaciones de cada opción
- Validar la conformidad de las soluciones seleccionadas con los requisitos de negocio
    - ■ Verificar que el proveedor cumple con estándares de seguridad y cumplimiento normativo requeridos
    - ■ Confirmar que la solución proporciona el nivel de servicio (SLA) necesario
    - ■ Evaluar la disponibilidad de soporte técnico y opciones de escalabilidad

■ Medios y recursos

- Matrices de evaluación de proveedores cloud
- Documentación de capacidades técnicas de AWS, Azure y GCP
- Estándares de cumplimiento normativo (ISO 27001, SOC 2, CIS Benchmarks)
- Herramientas de análisis de costes cloud (AWS Pricing Calculator, Azure Pricing Calculator, GCP Pricing Calculator)

■ Resultados esperados

- Matriz de evaluación de proveedores completada
- Recomendación documentada con justificación técnica y económica
- Análisis de conformidad con requisitos de seguridad y cumplimiento
- Documento de decisión firmado por stakeholders

Función 1: Diseño y Evaluación de Arquitecturas Cloud

Actividad 1.3 Seleccionar modelos de servicio cloud (IaaS, PaaS, SaaS, FaaS)

- Evaluar y recomendar el modelo de servicio cloud más adecuado para cada caso de uso empresarial
    - ■ Analizar las implicaciones técnicas de cada modelo (IaaS, PaaS, SaaS, FaaS)
    - ■ Evaluar las implicaciones económicas en términos de costes operativos y de inversión
    - ■ Considerar las implicaciones operativas en términos de responsabilidades de gestión
- Documentar la justificación de la elección del modelo de servicio
    - ■ Registrar los criterios de decisión y su ponderación
    - ■ Documentar las condiciones de revisión del modelo seleccionado
    - ■ Identificar los riesgos y limitaciones del modelo elegido
- Comunicar la recomendación a los responsables de decisión
    - ■ Presentar un análisis comparativo de los modelos evaluados
    - ■ Explicar las ventajas y desventajas de cada modelo en términos comprensibles para el negocio
    - ■ Proporcionar ejemplos de casos de uso similares

■ Medios y recursos

- Matriz de comparación de modelos de servicio (IaaS, PaaS, SaaS, FaaS)
- Documentación de características y limitaciones de cada modelo
- Herramientas de análisis de costes por modelo de servicio
- Casos de uso de referencia para cada modelo

■ Resultados esperados

- Recomendación de modelo de servicio documentada
- Análisis de implicaciones técnicas, económicas y operativas
- Matriz de decisión completada
- Documento de justificación aprobado por stakeholders

Función 1: Diseño y Evaluación de Arquitecturas Cloud

Actividad 1.4 Seleccionar modelos de despliegue cloud (público, privado, híbrido, multi-cloud)

- Determinar el modelo de despliegue cloud más apropiado en función de los requisitos de seguridad, cumplimiento, latencia y coste
  - ■ Analizar los requisitos de seguridad y cumplimiento normativo de la organización
  - ■ Evaluar los requisitos de latencia y rendimiento de las aplicaciones
  - ■ Considerar los requisitos de coste y flexibilidad operativa
- Elaborar comparativas técnicas de los modelos de despliegue
  - ■ Documentar las características técnicas de cada modelo (público, privado, híbrido, multi-cloud)
  - ■ Analizar las implicaciones de cada modelo en términos de control, seguridad y complejidad
  - ■ Evaluar la capacidad de cada modelo para soportar los requisitos de negocio
- Presentar recomendaciones a los responsables de decisión
  - ■ Elaborar un documento de recomendación que incluya análisis de ventajas y desventajas
  - ■ Proporcionar estimaciones de coste y esfuerzo de implementación
  - ■ Identificar los riesgos y mitigaciones asociados a cada modelo
- Revisar periódicamente la idoneidad del modelo de despliegue seleccionado
  - ■ Evaluar cambios en los requisitos de negocio que puedan afectar la decisión
  - ■ Monitorear la evolución de las capacidades de los proveedores cloud
  - ■ Proponer cambios en el modelo de despliegue si es necesario

■ Medios y recursos

- Matriz de comparación de modelos de despliegue
- Documentación de requisitos de seguridad y cumplimiento
- Herramientas de análisis de latencia y rendimiento
- Herramientas de análisis de costes por modelo de despliegue
- Marcos de referencia para evaluación de modelos de despliegue

■ Resultados esperados

- Recomendación de modelo de despliegue documentada
- Análisis de requisitos de seguridad, cumplimiento, latencia y coste
- Matriz de decisión completada
- Plan de revisión periódica del modelo seleccionado

Función 2: Provisión y Configuración de Infraestructura Cloud

Función 2: Provisión y Configuración de Infraestructura Cloud

Actividad 2.1 Provisionar servicios en plataformas cloud públicas

- Provisionar y configurar servicios en plataformas de cloud público (AWS, Azure, GCP) mediante consola, CLI o herramientas de IaC
  - ■ Utilizar la consola de administración del proveedor cloud para crear y configurar recursos
  - ■ Utilizar herramientas de línea de comandos (AWS CLI, Azure CLI, gcloud) para automatizar el aprovisionamiento
  - ■ Implementar infraestructura como código (IaC) utilizando herramientas como Terraform, CloudFormation o Pulumi
- Establecer grupos de seguridad, políticas de acceso y configuraciones de red
  - ■ Configurar grupos de seguridad y reglas de firewall para controlar el tráfico de red
  - ■ Definir políticas de acceso basadas en roles (RBAC) para los recursos cloud
  - ■ Configurar redes virtuales, subredes y tablas de enrutamiento
- Asegurar que los entornos cumplen con los estándares de la organización
  - ■ Validar que la configuración cumple con las políticas de seguridad de la organización
  - ■ Verificar que los recursos están etiquetados correctamente para gobernanza y seguimiento de costes
  - ■ Confirmar que la configuración de red y seguridad es consistente con los estándares

■ Medios y recursos

- Consolas de administración de AWS, Azure y GCP
- Herramientas de línea de comandos (AWS CLI, Azure CLI, gcloud)
- Herramientas de IaC (Terraform, CloudFormation, Pulumi)
- Documentación de estándares de configuración de la organización
- Plantillas de configuración de seguridad

■ Resultados esperados

- Servicios cloud aprovisionados y configurados correctamente
- Grupos de seguridad y políticas de acceso implementados
- Configuración de red validada y documentada
- Cumplimiento con estándares organizacionales verificado

Función 2: Provisión y Configuración de Infraestructura Cloud

Actividad 2.2 Desplegar infraestructuras cloud privadas

- Desplegar y configurar infraestructuras cloud privadas (on-premise o hosted) utilizando plataformas como OpenStack, VMware vCloud o Azure Stack
  - ■ Instalar y configurar la plataforma de cloud privada (OpenStack, VMware vCloud, Azure Stack)
  - ■ Configurar los componentes de infraestructura (cómputo, almacenamiento, red)
  - ■ Establecer la conectividad entre los componentes de la plataforma
- Definir redes virtuales, políticas de seguridad y recursos de cómputo y almacenamiento
  - ■ Crear redes virtuales y configurar el enrutamiento entre ellas
  - ■ Definir políticas de seguridad y grupos de seguridad para los recursos
  - ■ Provisionar recursos de cómputo (máquinas virtuales) y almacenamiento (volúmenes, almacenes de datos)

- Validar el correcto funcionamiento del entorno antes de su puesta en producción
  - ■ Realizar pruebas de conectividad entre componentes
  - ■ Verificar que los recursos de cómputo y almacenamiento funcionan correctamente
  - ■ Validar que las políticas de seguridad se aplican correctamente

■ Medios y recursos

- Plataformas de cloud privada (OpenStack, VMware vCloud, Azure Stack)
- Documentación de arquitectura de cloud privada
- Herramientas de gestión de cloud privada
- Equipamiento de infraestructura (servidores, almacenamiento, red)
- Plantillas de configuración de seguridad

■ Resultados esperados

- Plataforma de cloud privada instalada y configurada
- Redes virtuales, políticas de seguridad y recursos creados
- Validación de funcionamiento completada
- Documentación de configuración actualizada

Función 2: Provisión y Configuración de Infraestructura Cloud

Actividad 2.3 Configurar entornos cloud híbridos

- Diseñar e implementar arquitecturas que combinen recursos on-premise con servicios de cloud público
  - ■ Definir la distribución de cargas de trabajo entre entornos on-premise y cloud público
  - ■ Diseñar la arquitectura de integración entre entornos
  - ■ Documentar los flujos de datos y las dependencias entre entornos
- Garantizar la interoperabilidad y la coherencia de las políticas de seguridad
  - ■ Configurar conectividad segura entre entornos (VPN, ExpressRoute, Direct Connect)
  - ■ Aplicar políticas de seguridad consistentes en ambos entornos
  - ■ Validar que los datos se transmiten de forma segura entre entornos
- Validar la integración y el flujo de datos entre entornos
  - ■ Realizar pruebas de conectividad entre entornos on-premise y cloud
  - ■ Verificar que los datos se sincronizan correctamente entre entornos
  - ■ Validar que las aplicaciones funcionan correctamente en el entorno híbrido

■ Medios y recursos

- Herramientas de conectividad segura (VPN, ExpressRoute, Direct Connect)
- Plataformas de cloud público (AWS, Azure, GCP)
- Infraestructura on-premise
- Herramientas de gestión de identidades y accesos
- Documentación de políticas de seguridad

■ Resultados esperados

- Arquitectura de cloud híbrido diseñada y documentada
- Conectividad segura entre entornos establecida
- Políticas de seguridad coherentes implementadas
- Validación de integración completada

Función 2: Provisión y Configuración de Infraestructura Cloud

Actividad 2.4 Diseñar soluciones de red en entornos cloud

- Planificar y configurar la arquitectura de red cloud, incluyendo VPCs, subredes, tablas de enrutamiento, balanceadores de carga y gateways
  - ■ Diseñar el esquema de direccionamiento IP y la segmentación de redes
  - ■ Configurar VPCs (Virtual Private Clouds) y subredes
  - ■ Establecer tablas de enrutamiento y políticas de enrutamiento
- Diseñar topologías de red seguras y de alta disponibilidad para aplicaciones críticas
  - ■ Implementar balanceadores de carga para distribuir el tráfico
  - ■ Configurar gateways y puntos de acceso a la red
  - ■ Diseñar mecanismos de redundancia y failover
- Documentar la arquitectura de red y sus políticas de seguridad asociadas
  - ■ Crear diagramas de la arquitectura de red
  - ■ Documentar las políticas de seguridad y reglas de firewall
  - ■ Registrar las decisiones de diseño y su justificación

■ Medios y recursos

- Herramientas de diseño de red (Lucidchart, Draw.io, Visio)
- Consolas de administración de cloud (AWS, Azure, GCP)
- Herramientas de IaC para configuración de red
- Documentación de estándares de red de la organización
- Herramientas de análisis de tráfico de red

■ Resultados esperados

- Arquitectura de red cloud diseñada y documentada
- VPCs, subredes y tablas de enrutamiento configuradas
- Balanceadores de carga y gateways implementados
- Políticas de seguridad de red documentadas

Función 3: Automatización e Infraestructura como Código

Función 3: Automatización e Infraestructura como Código

Actividad 3.1 Desarrollar scripts y pipelines de automatización de infraestructura

- Desarrollar scripts y pipelines de automatización para el aprovisionamiento, configuración y gestión de recursos cloud
  - ■ Escribir scripts en lenguajes como Python, Bash o PowerShell para automatizar tareas de infraestructura
  - ■ Crear pipelines de automatización que orquesten múltiples pasos de aprovisionamiento y configuración
  - ■ Integrar herramientas de automatización en los flujos de trabajo existentes
- Reducir la intervención manual y los errores humanos
  - ■ Identificar tareas manuales repetitivas que pueden ser automatizadas
  - ■ Implementar validaciones y controles de calidad en los scripts de automatización
  - ■ Documentar los scripts y procedimientos de automatización
- Mantener y mejorar continuamente los scripts de automatización
  - ■ Revisar y actualizar los scripts cuando cambien los requisitos
  - ■ Monitorear la ejecución de los scripts y resolver problemas
  - ■ Implementar mejoras basadas en el feedback de los usuarios

■ Medios y recursos

- Lenguajes de scripting (Python, Bash, PowerShell)
- Herramientas de automatización (Ansible, Chef, Puppet)
- Sistemas de control de versiones (Git)
- Herramientas de CI/CD (Jenkins, GitLab CI, GitHub Actions)
- Documentación de APIs de proveedores cloud

■ Resultados esperados

- Scripts de automatización desarrollados y probados
- Pipelines de automatización implementados
- Reducción de intervención manual documentada
- Documentación de scripts y procedimientos completada

Función 3: Automatización e Infraestructura como Código

Actividad 3.2 Implementar herramientas de Infrastructure as Code (IaC)

- Utilizar herramientas de IaC (Terraform, Pulumi, CloudFormation) para definir y gestionar la infraestructura cloud
  - ■ Escribir código de infraestructura utilizando lenguajes de IaC (HCL, Python, YAML, JSON)
  - ■ Definir recursos cloud, redes, políticas de seguridad y configuraciones
  - ■ Versionar el código de infraestructura en repositorios de control de versiones
- Asegurar la coherencia de la configuración entre entornos
  - ■ Utilizar variables y módulos de IaC para reutilizar configuraciones
  - ■ Implementar validaciones de código de infraestructura
  - ■ Aplicar políticas de revisión de código para cambios de infraestructura
- Automatizar el despliegue de infraestructura
  - ■ Integrar herramientas de IaC en pipelines de CI/CD

■ Implementar procesos de aprobación para cambios de infraestructura
■ Automatizar la creación, actualización y eliminación de recursos

■ Medios y recursos

- Herramientas de IaC (Terraform, Pulumi, CloudFormation)
- Lenguajes de IaC (HCL, Python, YAML, JSON)
- Sistemas de control de versiones (Git)
- Herramientas de CI/CD (Jenkins, GitLab CI, GitHub Actions)
- Documentación de sintaxis y mejores prácticas de IaC

■ Resultados esperados

- Código de infraestructura escrito y versionado
- Recursos cloud definidos mediante IaC
- Coherencia de configuración entre entornos validada
- Despliegue automatizado de infraestructura implementado

Función 3: Automatización e Infraestructura como Código

Actividad 3.3 Gestionar configuración y detectar desviaciones (configuration drift)

- Mantener el control de la configuración de todos los servicios cloud desplegados
  ■ Utilizar herramientas de gestión de configuración (Ansible, Chef, Puppet) para aplicar configuraciones
  ■ Mantener repositorios de IaC actualizados con la configuración actual
  ■ Documentar los cambios de configuración y su justificación
- Asegurar la coherencia entre entornos (desarrollo, preproducción, producción)
  ■ Implementar procesos de sincronización de configuración entre entornos
  ■ Validar que la configuración es consistente en todos los entornos
  ■ Aplicar políticas de cambio de configuración
- Detectar y corregir desviaciones de configuración (configuration drift)
  ■ Utilizar herramientas de detección de configuration drift
  ■ Monitorear cambios no autorizados en la configuración
  ■ Implementar procesos de corrección automática o manual de desviaciones
- Auditar configuraciones cloud
  ■ Realizar auditorías periódicas de la configuración de recursos cloud
  ■ Generar informes de conformidad de configuración
  ■ Identificar y documentar desviaciones de políticas

■ Medios y recursos

- Herramientas de gestión de configuración (Ansible, Chef, Puppet)
- Herramientas de IaC (Terraform, CloudFormation, Pulumi)
- Herramientas de detección de configuration drift
- Sistemas de control de versiones (Git)
- Herramientas de auditoría de configuración

■ Resultados esperados

- Configuración de servicios cloud documentada
- Coherencia de configuración entre entornos validada
- Desviaciones de configuración detectadas y corregidas
- Auditoría de configuración completada

Función 4: Operación y Monitoreo de Servicios Cloud

Función 4: Operación y Monitoreo de Servicios Cloud

Actividad 4.1 Configurar herramientas de monitoreo y observabilidad

- Configurar y gestionar herramientas de monitoreo de rendimiento (APM, métricas de infraestructura, trazas distribuidas)
  - Instalar y configurar herramientas de APM (Application Performance Monitoring) como New Relic, Datadog o Dynatrace
  - Configurar la recopilación de métricas de infraestructura (CPU, memoria, disco, red)
  - Implementar trazas distribuidas para seguimiento de transacciones entre servicios
- Diseñar e implementar una estrategia de observabilidad integral
  - Combinar métricas, logs y trazas distribuidas (los tres pilares de la observabilidad)
  - Configurar herramientas como Prometheus, Grafana, Jaeger, ELK Stack o servicios nativos cloud
  - Asegurar que la observabilidad cubre los componentes críticos de la arquitectura
- Configurar dashboards y alertas de rendimiento
  - Crear dashboards que visualicen métricas clave de rendimiento
  - Configurar alertas para anomalías y degradación del servicio
  - Establecer umbrales de alerta basados en SLOs

Medios y recursos

- Herramientas de APM (New Relic, Datadog, Dynatrace, Elastic APM)
- Herramientas de monitoreo de infraestructura (Prometheus, Grafana, Zabbix)
- Herramientas de trazas distribuidas (Jaeger, Zipkin, AWS X-Ray)
- Herramientas de agregación de logs (ELK Stack, Splunk, CloudWatch)
- Documentación de métricas y alertas

Resultados esperados

- Herramientas de monitoreo configuradas e integradas
- Estrategia de observabilidad implementada
- Dashboards de rendimiento creados
- Alertas configuradas y validadas

Función 4: Operación y Monitoreo de Servicios Cloud

Actividad 4.2 Definir SLIs, SLOs y analizar tendencias de rendimiento

- Definir SLIs (Service Level Indicators) y SLOs (Service Level Objectives) para los servicios cloud
  - Identificar métricas clave que reflejen la experiencia del usuario (latencia, disponibilidad, tasa de error)
  - Establecer objetivos de nivel de servicio (SLOs) alineados con los requisitos de negocio
  - Documentar los SLIs y SLOs y comunicarlos a los equipos
- Analizar tendencias de rendimiento y proponer acciones de mejora proactiva
  - Recopilar y analizar datos históricos de rendimiento
  - Identificar tendencias de degradación o mejora
  - Proponer acciones de optimización basadas en el análisis
- Monitorear el cumplimiento de SLOs
  - Calcular regularmente el cumplimiento de SLOs
  - Generar informes de cumplimiento de SLOs

■ Identificar períodos de incumplimiento y analizar las causas

■ Medios y recursos

- Herramientas de monitoreo y análisis de rendimiento
- Plantillas de SLI/SLO
- Herramientas de análisis de datos (Grafana, Kibana, Tableau)
- Documentación de requisitos de negocio
- Herramientas de cálculo de error budget

■ Resultados esperados

- SLIs y SLOs definidos y documentados
- Análisis de tendencias de rendimiento completado
- Propuestas de mejora identificadas
- Informes de cumplimiento de SLOs generados

Función 4: Operación y Monitoreo de Servicios Cloud

Actividad 4.3 Gestionar incidentes y resolver problemas operativos

- Diagnosticar y resolver incidencias técnicas en plataformas cloud, siguiendo los procedimientos de gestión de incidentes (ITIL)
  - ■ Recibir y clasificar incidencias según su severidad
  - ■ Diagnosticar la causa raíz del problema
  - ■ Implementar soluciones y validar su efectividad
- Coordinar con los equipos de soporte del proveedor cloud cuando sea necesario
  - ■ Abrir tickets de soporte con el proveedor cloud
  - ■ Proporcionar información detallada sobre el problema
  - ■ Colaborar en la resolución del problema
- Documentar las incidencias, las causas raíz y las acciones correctivas
  - ■ Registrar los detalles de la incidencia en el sistema de tickets
  - ■ Documentar el análisis de causa raíz
  - ■ Registrar las acciones correctivas implementadas

■ Medios y recursos

- Sistema de gestión de incidentes (ITIL compatible)
- Herramientas de diagnóstico y troubleshooting
- Documentación de procedimientos de resolución
- Contactos de soporte del proveedor cloud
- Runbooks operativos

■ Resultados esperados

- Incidencias diagnosticadas y resueltas
- Tiempo medio de resolución (MTTR) reducido
- Documentación de causa raíz completada
- Acciones correctivas implementadas

Función 4: Operación y Monitoreo de Servicios Cloud

Actividad 4.4 Operar servicios empresariales en la nube

- Gestionar el ciclo de vida operativo de los servicios cloud en producción

    - Asegurar la disponibilidad continua de los servicios
    - Monitorear el rendimiento y la salud de los servicios
    - Realizar tareas operativas rutinarias (parcheo, actualizaciones, mantenimiento)
  - Asegurar el cumplimiento de los SLAs acordados
    - Monitorear el cumplimiento de SLAs
    - Tomar acciones correctivas cuando se detecten incumplimientos
    - Reportar el cumplimiento de SLAs a los stakeholders
  - Coordinar con los equipos de negocio para atender las necesidades operativas
    - Comunicarse regularmente con los responsables de negocio
    - Atender solicitudes de cambio y mejora
    - Resolver incidencias de primer y segundo nivel
  - Mantener actualizada la documentación operativa
    - Documentar procedimientos operativos estándar (SOPs)
    - Mantener runbooks actualizados
    - Registrar cambios en la configuración y la arquitectura

- **Medios y recursos**
  - Herramientas de monitoreo y alertas
  - Sistema de gestión de incidentes
  - Documentación de SLAs
  - Runbooks operativos
  - Herramientas de comunicación (Slack, Teams, email)

- **Resultados esperados**
  - Servicios operados con disponibilidad según SLA
  - SLAs cumplidos y reportados
  - Incidencias resueltas dentro de tiempos acordados
  - Documentación operativa actualizada

Función 5: Gestión de Servidores, Software y Contenedores

Función 5: Gestión de Servidores, Software y Contenedores

Actividad 5.1 Administrar instancias de cómputo cloud

- Administrar el ciclo de vida de instancias de cómputo cloud (VMs, instancias EC2, Azure VMs)
  - Provisionar nuevas instancias de cómputo según los requisitos
  - Configurar sistemas operativos y software base
  - Aplicar políticas de hardening y configuración segura
- Gestionar el parcheo y las actualizaciones de seguridad
  - Planificar y ejecutar parcheo de sistemas operativos
  - Aplicar actualizaciones de seguridad de forma oportuna
  - Validar que los parches no afecten la funcionalidad de las aplicaciones
- Monitorear el estado y el rendimiento de los servidores gestionados
  - Monitorear métricas de CPU, memoria, disco y red
  - Detectar y resolver problemas de rendimiento
  - Generar informes de estado de los servidores
- Descomisionar instancias de cómputo de forma segura
  - Realizar backup de datos antes de descomisionar
  - Eliminar datos sensibles de forma segura
  - Terminar la instancia y liberar recursos

Medios y recursos

- Consolas de administración de cloud (AWS, Azure, GCP)
- Herramientas de gestión de configuración (Ansible, Chef, Puppet)
- Herramientas de monitoreo de servidores
- Herramientas de parcheo automatizado
- Documentación de políticas de hardening

Resultados esperados

- Instancias de cómputo aprovisionadas y configuradas
- Políticas de hardening aplicadas
- Parcheo y actualizaciones de seguridad realizados
- Monitoreo de estado y rendimiento implementado

Función 5: Gestión de Servidores, Software y Contenedores

Actividad 5.2 Gestionar el ciclo de vida de aplicaciones y servicios software

- Administrar el despliegue, actualización y ciclo de vida de aplicaciones y servicios software en entornos cloud
  - Desplegar nuevas versiones de aplicaciones
  - Actualizar aplicaciones existentes de forma segura
  - Gestionar el versionado de aplicaciones
- Utilizar herramientas de gestión de configuración para aplicaciones
  - Utilizar Ansible, Chef o Puppet para automatizar la configuración de aplicaciones
  - Mantener la coherencia de configuración entre entornos
  - Documentar la configuración de aplicaciones
- Asegurar la coherencia de las versiones desplegadas

■ Mantener un registro de versiones desplegadas
■ Validar que las versiones son consistentes en todos los entornos
■ Implementar procesos de rollback si es necesario

■ **Medios y recursos**

• Herramientas de gestión de configuración (Ansible, Chef, Puppet)
• Herramientas de CI/CD (Jenkins, GitLab CI, GitHub Actions)
• Repositorios de artefactos (Artifactory, Nexus, Docker Registry)
• Herramientas de monitoreo de aplicaciones
• Documentación de procedimientos de despliegue

■ **Resultados esperados**

• Aplicaciones desplegadas y actualizadas
• Coherencia de versiones entre entornos validada
• Configuración de aplicaciones documentada
• Procesos de rollback implementados

Función 5: Gestión de Servidores, Software y Contenedores

Actividad 5.3 Administrar plataformas de orquestación de contenedores

• Desplegar, configurar y administrar plataformas de orquestación de contenedores (Kubernetes, EKS, AKS, GKE)
■ Instalar y configurar clústeres de Kubernetes
■ Configurar nodos de trabajo y componentes de control
■ Implementar políticas de seguridad y gestión de recursos
• Gestionar el ciclo de vida de los contenedores
■ Construir imágenes de contenedores
■ Registrar imágenes en repositorios (Docker Registry, ECR, ACR, GCR)
■ Desplegar y actualizar contenedores en el clúster
• Aplicar políticas de seguridad y gestión de recursos en clústeres
■ Configurar control de acceso basado en roles (RBAC)
■ Implementar políticas de seguridad de red
■ Establecer límites de recursos (CPU, memoria) para contenedores

■ **Medios y recursos**

• Plataformas de orquestación (Kubernetes, EKS, AKS, GKE)
• Herramientas de construcción de imágenes (Docker, Podman)
• Repositorios de imágenes (Docker Registry, ECR, ACR, GCR)
• Herramientas de gestión de Kubernetes (kubectl, Helm)
• Herramientas de monitoreo de contenedores

■ **Resultados esperados**

• Clústeres de Kubernetes instalados y configurados
• Imágenes de contenedores construidas y registradas
• Contenedores desplegados y orquestados
• Políticas de seguridad y gestión de recursos implementadas

Función 6: Integración de Sistemas y Arquitecturas de Mensajería

Función 6: Integración de Sistemas y Arquitecturas de Mensajería

Actividad 6.1 Integrar servicios cloud con sistemas existentes

- Diseñar e implementar integraciones entre servicios cloud y sistemas legados o de terceros
  - Utilizar APIs para conectar servicios cloud con sistemas externos
  - Implementar colas de mensajes para comunicación asíncrona
  - Utilizar buses de eventos para arquitecturas basadas en eventos
- Garantizar la compatibilidad, la seguridad y el rendimiento de las integraciones
  - Validar que los datos se transmiten correctamente entre sistemas
  - Implementar mecanismos de seguridad (autenticación, cifrado)
  - Optimizar el rendimiento de las integraciones
- Documentar los flujos de integración y los contratos de API
  - Crear diagramas de flujo de integración
  - Documentar las APIs utilizadas
  - Registrar los contratos de datos entre sistemas

■ Medios y recursos

- Herramientas de integración (MuleSoft, Apache Camel, AWS AppSync)
- Herramientas de gestión de APIs (Apigee, AWS API Gateway, Azure API Management)
- Herramientas de monitoreo de integraciones
- Documentación de APIs de sistemas legados
- Herramientas de prueba de integraciones

■ Resultados esperados

- Integraciones diseñadas e implementadas
- Compatibilidad entre sistemas validada
- Seguridad de integraciones implementada
- Documentación de flujos de integración completada

Función 6: Integración de Sistemas y Arquitecturas de Mensajería

Actividad 6.2 Implementar soluciones de mensajería y eventos en cloud

- Diseñar e implementar arquitecturas basadas en eventos y mensajería asíncrona
  - Utilizar servicios de mensajería cloud (AWS SQS/SNS, Azure Service Bus, Google Pub/Sub)
  - Implementar patrones de mensajería (publish-subscribe, request-reply, event sourcing)
  - Configurar tópicos, colas y suscripciones
- Configurar los flujos de mensajes, las políticas de reintentos y los mecanismos de gestión de errores
  - Definir políticas de reintentos para mensajes fallidos
  - Implementar mecanismos de dead-letter queues
  - Configurar timeouts y límites de reintentos
- Monitorear el rendimiento y la salud de los servicios de mensajería
  - Monitorear el número de mensajes en colas
  - Detectar y resolver problemas de entrega de mensajes
  - Generar informes de rendimiento de mensajería

■ **Medios y recursos**

- Servicios de mensajería cloud (AWS SQS/SNS, Azure Service Bus, Google Pub/Sub, Apache Kafka)
- Herramientas de monitoreo de mensajería
- Herramientas de prueba de mensajería
- Documentación de patrones de mensajería
- Herramientas de análisis de rendimiento

■ **Resultados esperados**

- Arquitecturas basadas en eventos diseñadas e implementadas
- Servicios de mensajería configurados
- Políticas de reintentos y gestión de errores implementadas
- Monitoreo de mensajería implementado

Función 7: Seguridad Cloud y Cumplimiento Normativo

Función 7: Seguridad Cloud y Cumplimiento Normativo

Actividad 7.1 Aplicar buenas prácticas de desarrollo seguro en cloud

- Integrar principios de seguridad en el ciclo de vida del desarrollo de software (SDLC) cloud
  - ■ Aplicar metodologías como DevSecOps y Secure by Design
  - ■ Integrar controles de seguridad en cada fase del SDLC
  - ■ Capacitar a los equipos de desarrollo en prácticas seguras
- Revisar el código fuente en busca de vulnerabilidades de seguridad
  - ■ Utilizar herramientas SAST (Static Application Security Testing) para análisis de código
  - ■ Realizar revisiones de código enfocadas en seguridad
  - ■ Documentar y priorizar las vulnerabilidades encontradas
- Promover el uso de librerías y dependencias seguras
  - ■ Mantener un registro de dependencias utilizadas
  - ■ Monitorear vulnerabilidades en dependencias
  - ■ Actualizar dependencias de forma oportuna

■ Medios y recursos

- Herramientas SAST (SonarQube, Checkmarx, Fortify)
- Herramientas de análisis de dependencias (Snyk, Dependabot, WhiteSource)
- Herramientas de gestión de secretos
- Documentación de estándares de codificación segura
- Herramientas de CI/CD con integración de seguridad

■ Resultados esperados

- Principios de seguridad integrados en SDLC
- Vulnerabilidades de código identificadas y corregidas
- Dependencias seguras utilizadas
- Capacitación en prácticas seguras completada

Función 7: Seguridad Cloud y Cumplimiento Normativo

Actividad 7.2 Definir e implementar controles de seguridad cloud

- Definir el modelo de seguridad compartida en entornos cloud
  - ■ Documentar las responsabilidades de seguridad del proveedor y de la organización
  - ■ Establecer controles preventivos, detectivos y correctivos
  - ■ Alinear el modelo de seguridad con los requisitos de negocio
- Implementar controles técnicos de seguridad
  - ■ Implementar cifrado en tránsito y en reposo
  - ■ Configurar gestión de secretos (AWS Secrets Manager, Azure Key Vault, Google Secret Manager)
  - ■ Implementar Web Application Firewall (WAF) y firewalls de red
- Configurar segmentación de redes virtuales
  - ■ Diseñar zonas de seguridad (DMZ, aplicaciones, datos)
  - ■ Implementar políticas de firewall entre zonas
  - ■ Validar la segmentación de redes

■ Medios y recursos

• Servicios de seguridad cloud (AWS Security Hub, Azure Security Center, Google Cloud Security Command Center)
• Herramientas de gestión de secretos
• Herramientas de cifrado
• Firewalls y WAF
• Documentación de estándares de seguridad

■ **Resultados esperados**

• Modelo de seguridad compartida definido
• Controles técnicos de seguridad implementados
• Cifrado en tránsito y en reposo configurado
• Segmentación de redes implementada

Función 7: Seguridad Cloud y Cumplimiento Normativo

Actividad 7.3 Administrar identidades y accesos en la nube

• Gestionar el ciclo de vida de identidades, roles y permisos en entornos cloud
  ■ Utilizar servicios IAM (AWS IAM, Azure AD, GCP IAM) para gestionar identidades
  ■ Crear y gestionar roles y políticas de acceso
  ■ Implementar el ciclo de vida de identidades (provisioning, deprovisioning)
• Aplicar el principio de mínimo privilegio
  ■ Asignar permisos mínimos necesarios para cada rol
  ■ Revisar periódicamente los permisos asignados
  ■ Eliminar permisos innecesarios
• Implementar políticas de acceso condicional
  ■ Configurar autenticación multifactor (MFA)
  ■ Implementar políticas de acceso basadas en ubicación, dispositivo o tiempo
  ■ Monitorear intentos de acceso sospechosos
• Auditar periódicamente los accesos y generar informes de cumplimiento
  ■ Realizar auditorías de acceso regularmente
  ■ Generar informes de cumplimiento de políticas de acceso
  ■ Identificar y corregir accesos no autorizados

■ **Medios y recursos**

• Servicios IAM (AWS IAM, Azure AD, GCP IAM)
• Herramientas de gestión de identidades (Okta, Ping Identity, Azure AD)
• Herramientas de auditoría de acceso
• Herramientas de autenticación multifactor
• Documentación de políticas de acceso

■ **Resultados esperados**

• Identidades, roles y permisos gestionados
• Principio de mínimo privilegio aplicado
• Acceso condicional implementado
• Auditoría de acceso completada

Función 7: Seguridad Cloud y Cumplimiento Normativo

Actividad 7.4 Identificar y mitigar vulnerabilidades de seguridad

- Realizar análisis de vulnerabilidades y pruebas de penetración en aplicaciones desplegadas en la nube
  - ■ Utilizar herramientas especializadas (OWASP ZAP, Burp Suite, Trivy) para análisis de vulnerabilidades
  - ■ Realizar pruebas de penetración periódicas
  - ■ Documentar las vulnerabilidades encontradas
- Clasificar las vulnerabilidades encontradas según su criticidad
  - ■ Utilizar escalas de severidad (CVSS) para clasificar vulnerabilidades
  - ■ Priorizar las vulnerabilidades según su impacto
  - ■ Establecer plazos de remediación según la severidad
- Elaborar informes de hallazgos y proponer acciones correctivas
  - ■ Documentar las vulnerabilidades en informes detallados
  - ■ Proponer soluciones para cada vulnerabilidad
  - ■ Priorizar las acciones correctivas
- Evaluar riesgos de seguridad en código
  - ■ Revisar el código fuente para identificar riesgos como inyecciones y exposición de credenciales
  - ■ Utilizar herramientas de análisis estático y dinámico (SAST/DAST)
  - ■ Documentar los riesgos identificados

■ **Medios y recursos**

- Herramientas de análisis de vulnerabilidades (OWASP ZAP, Burp Suite, Trivy, Nessus)
- Herramientas SAST/DAST (SonarQube, Checkmarx, Fortify)
- Herramientas de gestión de vulnerabilidades
- Documentación de escalas de severidad (CVSS)
- Herramientas de prueba de penetración

■ **Resultados esperados**

- Análisis de vulnerabilidades completado
- Vulnerabilidades clasificadas según severidad
- Informes de hallazgos elaborados
- Acciones correctivas propuestas y priorizadas

Función 7: Seguridad Cloud y Cumplimiento Normativo

Actividad 7.5 Asegurar cumplimiento normativo y promover cultura de seguridad

- Asegurar que los entornos cloud cumplen con las regulaciones y normativas aplicables
  - ■ Implementar controles para cumplir con GDPR, ENS, PCI-DSS, HIPAA y otras regulaciones
  - ■ Colaborar con equipos de compliance para preparar auditorías externas
  - ■ Mantener documentación de cumplimiento actualizada
- Implementar controles técnicos y organizativos de seguridad
  - ■ Configurar controles de acceso y cifrado según requisitos normativos
  - ■ Implementar procedimientos de auditoría y logging
  - ■ Establecer políticas de retención de datos
- Promover una cultura de seguridad cloud en la organización
  - ■ Facilitar sesiones de formación en seguridad cloud
  - ■ Elaborar guías y checklists de seguridad
  - ■ Actuar como referente interno en materia de seguridad cloud
- Mitigar vulnerabilidades en flujos DevOps
  - ■ Identificar y corregir vulnerabilidades en pipelines CI/CD
  - ■ Implementar controles de seguridad en fases de pipeline (build, test, deploy)
  - ■ Asegurar la integridad de artefactos y cadena de suministro de software

■ **Medios y recursos**

- Herramientas de cumplimiento normativo (Compliance Manager, Azure Compliance Manager)
- Herramientas de auditoría y logging
- Documentación de regulaciones (GDPR, ENS, PCI-DSS, HIPAA)
- Herramientas de seguridad en CI/CD
- Materiales de formación en seguridad cloud

■ **Resultados esperados**

- Cumplimiento normativo implementado
- Controles técnicos y organizativos establecidos
- Auditorías externas superadas
- Cultura de seguridad promovida en la organización

Función 8: Almacenamiento, Datos y Bases de Datos Cloud

Función 8: Almacenamiento, Datos y Bases de Datos Cloud

Actividad 8.1 Diseñar soluciones de almacenamiento cloud

- Definir la arquitectura de almacenamiento cloud más adecuada
  - ■ Seleccionar tipos de almacenamiento (object storage, block storage, file storage) según requisitos
  - ■ Evaluar opciones de bases de datos gestionadas (RDS, Azure SQL, Cloud SQL, DynamoDB, Cosmos DB)
  - ■ Documentar la solución de almacenamiento
- Diseñar políticas de ciclo de vida de datos, replicación y archivado
  - ■ Definir políticas de retención de datos
  - ■ Configurar replicación para alta disponibilidad
  - ■ Implementar estrategias de archivado para datos históricos
- Asegurar el rendimiento, durabilidad y coste de la solución
  - ■ Optimizar el rendimiento de acceso a datos
  - ■ Garantizar la durabilidad de los datos
  - ■ Minimizar los costes de almacenamiento

■ Medios y recursos

- Servicios de almacenamiento cloud (S3, Azure Blob Storage, Google Cloud Storage)
- Servicios de bases de datos gestionadas (RDS, Azure SQL, Cloud SQL, DynamoDB, Cosmos DB)
- Herramientas de análisis de almacenamiento
- Documentación de opciones de almacenamiento
- Herramientas de monitoreo de almacenamiento

■ Resultados esperados

- Arquitectura de almacenamiento diseñada
- Tipos de almacenamiento seleccionados
- Políticas de ciclo de vida implementadas
- Solución documentada y validada

Función 8: Almacenamiento, Datos y Bases de Datos Cloud

Actividad 8.2 Administrar bases de datos en la nube

- Administrar el ciclo de vida de bases de datos gestionadas en cloud
  - ■ Provisionar bases de datos gestionadas (RDS, Azure SQL, Cloud SQL, DynamoDB, Cosmos DB)
  - ■ Configurar parámetros de base de datos
  - ■ Aplicar parcheo y actualizaciones de versión
- Diseñar estrategias de alta disponibilidad y replicación
  - ■ Configurar replicación de bases de datos
  - ■ Implementar failover automático
  - ■ Diseñar estrategias de backup y recuperación
- Optimizar el rendimiento de bases de datos
  - ■ Monitorear métricas de rendimiento
  - ■ Optimizar índices y consultas
  - ■ Escalar recursos según demanda

■ **Medios y recursos**

- Servicios de bases de datos gestionadas (RDS, Azure SQL, Cloud SQL, DynamoDB, Cosmos DB)
- Herramientas de monitoreo de bases de datos
- Herramientas de optimización de consultas
- Herramientas de backup y recuperación
- Documentación de mejores prácticas de bases de datos

■ **Resultados esperados**

- Bases de datos gestionadas aprovisionadas y configuradas
- Alta disponibilidad y replicación implementadas
- Rendimiento optimizado
- Estrategias de backup y recuperación establecidas

Función 8: Almacenamiento, Datos y Bases de Datos Cloud

Actividad 8.3 Migrar datos a la nube

- Diseñar y ejecutar procesos de migración de datos hacia servicios de almacenamiento y bases de datos cloud
  - ■ Planificar la estrategia de migración de datos
  - ■ Seleccionar herramientas de migración (AWS DMS, Azure Data Factory, Google Cloud Dataflow)
  - ■ Ejecutar la migración de datos
- Garantizar la integridad, confidencialidad y disponibilidad de los datos durante la migración
  - ■ Implementar cifrado durante la transferencia de datos
  - ■ Validar la integridad de los datos migrados
  - ■ Minimizar el tiempo de inactividad
- Validar la consistencia de los datos migrados mediante pruebas
  - ■ Realizar pruebas de validación de datos
  - ■ Comparar datos origen y destino
  - ■ Documentar los resultados de validación

■ **Medios y recursos**

- Herramientas de migración de datos (AWS DMS, Azure Data Factory, Google Cloud Dataflow)
- Herramientas de validación de datos
- Herramientas de cifrado de datos
- Documentación de estrategias de migración
- Herramientas de monitoreo de migración

■ **Resultados esperados**

- Estrategia de migración de datos diseñada
- Datos migrados a cloud
- Integridad de datos validada
- Documentación de migración completada

Función 9: Continuidad, Recuperación y Copias de Seguridad

Función 9: Continuidad, Recuperación y Copias de Seguridad

Actividad 9.1 Diseñar planes de continuidad y recuperación ante desastres

- Diseñar e implementar planes de continuidad de negocio (BCP) y recuperación ante desastres (DRP)
  - ■ Identificar servicios críticos y su impacto en el negocio
  - ■ Definir estrategias de recuperación para cada servicio
  - ■ Documentar los planes de continuidad y recuperación
- Definir objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO)
  - ■ Establecer RTO y RPO para cada servicio crítico
  - ■ Alinear RTO y RPO con requisitos de negocio
  - ■ Documentar los objetivos de recuperación
- Realizar pruebas periódicas de los planes
  - ■ Ejecutar simulacros de recuperación
  - ■ Validar que los planes funcionan correctamente
  - ■ Documentar los resultados de las pruebas

■ Medios y recursos

- Herramientas de planificación de continuidad
- Herramientas de backup y recuperación
- Documentación de planes de continuidad
- Herramientas de simulación de desastres
- Documentación de RTO y RPO

■ Resultados esperados

- Planes de continuidad de negocio diseñados
- Planes de recuperación ante desastres implementados
- RTO y RPO definidos
- Pruebas de planes completadas

Función 9: Continuidad, Recuperación y Copias de Seguridad

Actividad 9.2 Implementar políticas y procedimientos de backup

- Diseñar e implementar políticas y procedimientos de backup para datos y servicios cloud
  - ■ Definir frecuencias de backup (diaria, semanal, mensual)
  - ■ Seleccionar destinos de almacenamiento de backups
  - ■ Automatizar los procesos de copia de seguridad
- Definir retenciones y destinos de almacenamiento
  - ■ Establecer políticas de retención de backups
  - ■ Seleccionar opciones de almacenamiento (local, geográficamente distribuido)
  - ■ Implementar archivado de backups antiguos
- Verificar la correcta ejecución de los backups
  - ■ Monitorear la ejecución de backups
  - ■ Validar la integridad de los backups
  - ■ Generar informes de estado de backups

■ Medios y recursos

- Herramientas de backup cloud (AWS Backup, Azure Backup, Google Cloud Backup)
- Herramientas de automatización de backups
- Herramientas de monitoreo de backups
- Documentación de políticas de backup
- Herramientas de validación de integridad

■ Resultados esperados

- Políticas de backup diseñadas e implementadas
- Procesos de backup automatizados
- Retenciones de backup configuradas
- Validación de integridad de backups completada

Función 9: Continuidad, Recuperación y Copias de Seguridad

Actividad 9.3 Restaurar servicios tras incidentes cloud

- Ejecutar los procedimientos de restauración de servicios y datos cloud tras incidentes o desastres
  - ■ Activar el plan de recuperación ante desastres
  - ■ Restaurar datos desde backups
  - ■ Restaurar servicios en el entorno de recuperación
- Coordinar con los equipos técnicos y de negocio para minimizar el tiempo de inactividad
  - ■ Comunicar el estado de la recuperación a los stakeholders
  - ■ Coordinar las actividades de restauración
  - ■ Minimizar el impacto en el negocio
- Validar la integridad y funcionalidad de los servicios restaurados
  - ■ Realizar pruebas de funcionalidad de servicios restaurados
  - ■ Validar la integridad de los datos restaurados
  - ■ Documentar los resultados de validación

■ Medios y recursos

- Planes de recuperación ante desastres
- Herramientas de restauración de datos
- Herramientas de monitoreo de recuperación
- Documentación de procedimientos de restauración
- Herramientas de validación de integridad

■ Resultados esperados

- Servicios restaurados tras incidente
- Datos restaurados correctamente
- Integridad de servicios validada
- Documentación de restauración completada

Función 10: Migración de Aplicaciones y Adopción Cloud

Función 10: Migración de Aplicaciones y Adopción Cloud

Actividad 10.1 Planificar y ejecutar migraciones de aplicaciones

- Planificar y ejecutar la migración de aplicaciones desde entornos on-premise o legacy hacia la nube
  - ■ Evaluar aplicaciones candidatas para migración
  - ■ Seleccionar la estrategia de migración más adecuada (rehost, replatform, refactor)
  - ■ Planificar el cronograma y los recursos de migración
- Aplicar la estrategia de migración más adecuada
  - ■ Ejecutar la migración según la estrategia seleccionada
  - ■ Configurar la aplicación en el entorno cloud
  - ■ Validar que la aplicación funciona correctamente
- Realizar pruebas de validación post-migración
  - ■ Ejecutar pruebas funcionales de la aplicación
  - ■ Validar el rendimiento de la aplicación
  - ■ Documentar los resultados de las pruebas
- Gestionar los riesgos de migración
  - ■ Identificar riesgos potenciales de migración
  - ■ Implementar mitigaciones de riesgos
  - ■ Monitorear la ejecución de la migración

■ Medios y recursos

- Herramientas de evaluación de aplicaciones
- Herramientas de migración de aplicaciones (AWS Application Migration Service, Azure Migrate)
- Herramientas de prueba de aplicaciones
- Documentación de estrategias de migración
- Herramientas de monitoreo de migración

■ Resultados esperados

- Aplicaciones evaluadas para migración
- Estrategia de migración seleccionada
- Aplicaciones migradas a cloud
- Pruebas de validación completadas

Función 10: Migración de Aplicaciones y Adopción Cloud

Actividad 10.2 Definir estrategias de adopción cloud

- Elaborar el plan estratégico de transición hacia la nube
  - ■ Identificar los workloads candidatos para migración a cloud
  - ■ Seleccionar el modelo de adopción más adecuado (lift-and-shift, re-platforming, re-architecting)
  - ■ Documentar la estrategia de adopción
- Establecer hitos, KPIs y criterios de éxito
  - ■ Definir hitos del proyecto de adopción cloud
  - ■ Establecer KPIs para medir el éxito
  - ■ Alinear criterios de éxito con objetivos de negocio
- Comunicar la hoja de ruta de adopción cloud
  - ■ Presentar la estrategia a los stakeholders

- Comunicar los beneficios esperados
- Obtener apoyo de la dirección

■ Medios y recursos

- Marcos de referencia de adopción cloud (AWS CAF, Azure CAF, Google Cloud Adoption Framework)
- Herramientas de evaluación de workloads
- Documentación de modelos de adopción
- Herramientas de planificación de proyectos
- Herramientas de análisis de KPIs

■ Resultados esperados

- Plan estratégico de adopción cloud elaborado
- Workloads candidatos identificados
- Modelo de adopción seleccionado
- Hitos, KPIs y criterios de éxito definidos

Función 10: Migración de Aplicaciones y Adopción Cloud

Actividad 10.3 Gestionar cambios organizativos y capacitación en adopción cloud

- Impulsar la transformación cultural y organizativa necesaria para la adopción cloud
  - Identificar resistencias al cambio
  - Diseñar estrategias de gestión del cambio
  - Promover nuevas formas de trabajo basadas en cloud
- Gestionar la resistencia al cambio
  - Comunicar los beneficios de la adopción cloud
  - Involucrar a los equipos en el proceso de cambio
  - Proporcionar apoyo durante la transición
- Diseñar programas de formación y capacitación para los equipos afectados
  - Identificar necesidades de formación
  - Diseñar programas de capacitación
  - Ejecutar sesiones de formación
- Actuar como agente de cambio y referente interno en materia cloud
  - Liderar iniciativas de transformación cloud
  - Proporcionar orientación y mentoría
  - Promover mejores prácticas cloud

■ Medios y recursos

- Marcos de referencia de gestión del cambio
- Herramientas de comunicación
- Programas de formación en cloud
- Materiales de capacitación
- Herramientas de seguimiento de adopción

■ Resultados esperados

- Estrategia de gestión del cambio implementada
- Resistencias al cambio identificadas y mitigadas
- Programas de formación diseñados e implementados
- Adopción cloud acelerada en la organización

Función 11: Optimización de Costes y Recursos Cloud

Función 11: Optimización de Costes y Recursos Cloud

Actividad 11.1 Analizar uso de recursos y optimizar infraestructura cloud

- Analizar el uso de recursos cloud para identificar oportunidades de optimización
  - ■ Recopilar datos de uso de recursos
  - ■ Analizar patrones de utilización
  - ■ Identificar recursos subutilizados u ociosos
- Aplicar técnicas de rightsizing y gestión de instancias
  - ■ Redimensionar instancias según demanda real
  - ■ Utilizar instancias reservadas para cargas predecibles
  - ■ Utilizar instancias spot para cargas flexibles
- Eliminar recursos ociosos
  - ■ Identificar recursos no utilizados
  - ■ Validar que pueden ser eliminados
  - ■ Eliminar recursos de forma segura

■ Medios y recursos

- Herramientas de análisis de costes cloud (AWS Cost Explorer, Azure Cost Management, Google Cloud Cost Management)
- Herramientas de monitoreo de recursos
- Herramientas de rightsizing (Compute Optimizer, Azure Advisor)
- Documentación de opciones de instancias
- Herramientas de análisis de patrones de uso

■ Resultados esperados

- Análisis de uso de recursos completado
- Oportunidades de optimización identificadas
- Rightsizing implementado
- Recursos ociosos eliminados

Función 11: Optimización de Costes y Recursos Cloud

Actividad 11.2 Gestionar costes y presupuestos cloud

- Monitorear y controlar el gasto en servicios cloud
  - ■ Establecer presupuestos por servicio y departamento
  - ■ Configurar alertas de coste
  - ■ Monitorear el gasto en tiempo real
- Aplicar prácticas de FinOps
  - ■ Implementar políticas de gobernanza financiera
  - ■ Asignar costes a centros de coste
  - ■ Promover la responsabilidad financiera
- Analizar las facturas de los proveedores cloud
  - ■ Revisar facturas de proveedores cloud
  - ■ Identificar cargos inesperados
  - ■ Validar la precisión de los cargos
- Elaborar informes de coste y presentar recomendaciones de optimización

■ Generar informes de coste por servicio
■ Analizar tendencias de coste
■ Proponer acciones de optimización

■ **Medios y recursos**

• Herramientas de gestión de costes cloud (AWS Cost Management, Azure Cost Management, Google Cloud Cost Management)
• Herramientas de análisis de facturas
• Herramientas de presupuestación
• Documentación de opciones de ahorro de costes
• Herramientas de análisis de ROI

■ **Resultados esperados**

• Presupuestos establecidos y monitoreados
• Alertas de coste configuradas
• Facturas analizadas
• Recomendaciones de optimización presentadas

Función 12: Gestión de Proyectos, Documentación y Comunicación Cloud

Función 12: Gestión de Proyectos, Documentación y Comunicación Cloud

Actividad 12.1 Coordinar y seguimiento de proyectos cloud

- Monitorear el avance de los proyectos cloud respecto al plan establecido
  - ■ Seguimiento de plazos y cronograma
  - ■ Monitoreo de costes del proyecto
  - ■ Validación del alcance del proyecto
- Identificar desviaciones en plazos, costes y alcance
  - ■ Detectar desviaciones significativas
  - ■ Analizar las causas de las desviaciones
  - ■ Proponer acciones correctivas
- Actualizar los registros de seguimiento y comunicar el estado del proyecto
  - ■ Mantener registros de seguimiento actualizados
  - ■ Comunicar el estado a los stakeholders
  - ■ Generar informes de avance
- Proponer acciones correctivas cuando se detecten desviaciones significativas
  - ■ Identificar opciones de corrección
  - ■ Evaluar el impacto de cada opción
  - ■ Implementar acciones correctivas

■ Medios y recursos

- Herramientas de gestión de proyectos (Jira, Azure DevOps, Monday.com)
- Herramientas de seguimiento de cronograma
- Herramientas de análisis de desviaciones
- Documentación de planes de proyecto
- Herramientas de comunicación

■ Resultados esperados

- Seguimiento de proyectos implementado
- Desviaciones identificadas y analizadas
- Registros de seguimiento actualizados
- Acciones correctivas implementadas

Función 12: Gestión de Proyectos, Documentación y Comunicación Cloud

Actividad 12.2 Documentar configuraciones y decisiones de arquitectura cloud

- Elaborar y mantener actualizada la documentación técnica de las arquitecturas cloud desplegadas
  - ■ Crear diagramas de infraestructura
  - ■ Documentar configuraciones de servicios
  - ■ Mantener documentación actualizada
- Documentar decisiones arquitectónicas (ADRs) y runbooks operativos
  - ■ Registrar decisiones arquitectónicas y su justificación
  - ■ Crear runbooks para procedimientos operativos
  - ■ Documentar procedimientos de troubleshooting

- Asegurar que la documentación es accesible y comprensible para todos los equipos
  - ■ Utilizar formatos estándar de documentación
  - ■ Mantener documentación en repositorios centralizados
  - ■ Revisar documentación regularmente
- Revisar la documentación periódicamente
  - ■ Actualizar documentación cuando cambia la arquitectura
  - ■ Validar que la documentación es precisa
  - ■ Obtener feedback de los usuarios

■ Medios y recursos

- Herramientas de documentación (Confluence, GitBook, Notion)
- Herramientas de diagramación (Lucidchart, Draw.io, Visio)
- Plantillas de documentación
- Sistemas de control de versiones (Git)
- Herramientas de colaboración

■ Resultados esperados

- Documentación técnica de arquitectura completada
- Decisiones arquitectónicas documentadas
- Runbooks operativos creados
- Documentación accesible y actualizada

Función 12: Gestión de Proyectos, Documentación y Comunicación Cloud

Actividad 12.3 Comunicar estado operativo y facilitar colaboración en iniciativas cloud

- Elaborar y presentar informes periódicos sobre el estado operativo de los servicios cloud
  - ■ Recopilar métricas de disponibilidad, rendimiento, seguridad y costes
  - ■ Analizar tendencias y anomalías
  - ■ Generar informes ejecutivos
- Adaptar el nivel de detalle y el formato del informe al público destinatario
  - ■ Crear informes técnicos para equipos de operaciones
  - ■ Crear informes ejecutivos para la dirección
  - ■ Utilizar visualizaciones claras y comprensibles
- Proponer acciones de mejora basadas en el análisis
  - ■ Identificar áreas de mejora
  - ■ Proponer iniciativas de optimización
  - ■ Priorizar acciones de mejora
- Gestionar la relación con clientes internos y externos, empleados y socios en iniciativas cloud
  - ■ Participar en reuniones de seguimiento
  - ■ Facilitar workshops y sesiones de co-creación
  - ■ Actuar como punto de contacto técnico
- Aplicar metodologías ágiles en proyectos cloud
  - ■ Participar en ceremonias ágiles (sprint planning, daily, retrospectivas)
  - ■ Promover la mejora continua
  - ■ Facilitar la entrega incremental de valor

■ Medios y recursos

- Herramientas de análisis de datos (Grafana, Kibana, Tableau, Power BI)
- Herramientas de generación de informes
- Herramientas de comunicación (Slack, Teams, email)

- Herramientas de gestión ágil (Jira, Azure DevOps)
- Documentación de métricas y KPIs

■ **Resultados esperados**

- Informes de estado operativo generados
- Métricas de disponibilidad, rendimiento, seguridad y costes reportadas
- Acciones de mejora propuestas
- Colaboración con stakeholders facilitada

ANEXO III Marco de competencias

Bloque 1 - Diseño y Evaluación de Arquitecturas Cloud

Objetivo pedagógico

Capacitar al profesional para diseñar arquitecturas cloud escalables y resilientes, evaluando proveedores y alineando soluciones con objetivos empresariales.

Actividades

Actividad 1.1 Diseñar arquitecturas cloud escalables y resilientes
Actividad 1.2 Evaluar proveedores y servicios cloud
Actividad 1.3 Seleccionar modelos de servicio cloud (IaaS, PaaS, SaaS, FaaS)
Actividad 1.4 Seleccionar modelos de despliegue cloud (público, privado, híbrido, multi-cloud)

Competencias

Competencias	Indicadores
C10 - Diseñar arquitecturas cloud híbridas estableciendo conectividad segura entre entornos on-premises y cloud para mantener flexibilidad operativa	Configuración de conexiones seguras (VPN, ExpressRoute, Direct Connect) con redundancia y failover automático Validación de latencia, ancho de banda y seguridad en comunicaciones entre entornos mediante pruebas de rendimiento Documentación de topología de red híbrida con políticas de enrutamiento, firewall y segmentación

Saberes asociados

Patrones Arquitectónicos Modernos

Microservicios

- Descomposición de aplicaciones monolíticas
- Comunicación entre servicios
- Gestión de transacciones distribuidas
- Versionado de APIs

Arquitectura Serverless

- Funciones como servicio (FaaS)
- Orquestación de flujos sin servidor
- Gestión de estado en aplicaciones serverless
- Optimización de costes en serverless

Arquitectura basada en Contenedores

- Contenedores Docker
- Orquestación con Kubernetes
- Gestión de imágenes de contenedor

- Redes de contenedores

Patrones de Resiliencia

- Circuit breaker
- Retry y backoff exponencial
- Bulkhead pattern
- Fallback y degradación elegante

Escalabilidad y Rendimiento en Cloud

Principios de Escalabilidad

- Escalado horizontal vs vertical
- Elasticidad y auto-escalado
- Balanceo de carga
- Particionamiento de datos (sharding)

Análisis de Rendimiento

- Identificación de cuellos de botella
- Optimización de latencia
- Throughput y capacidad
- Profiling de aplicaciones

Disponibilidad y Redundancia

- Replicación de datos
- Failover automático
- Zonas de disponibilidad
- Regiones geográficas

Evaluación de Proveedores Cloud

Análisis Técnico de Proveedores

- Capacidades de servicios (AWS, Azure, GCP)
- Modelos de precios y costes
- Disponibilidad de regiones y zonas
- Límites de servicio y cuotas

Cumplimiento Normativo y Certificaciones

- Certificaciones ISO 27001, SOC 2
- Cumplimiento GDPR, HIPAA, PCI-DSS
- Residencia de datos y soberanía
- Auditorías y reportes de cumplimiento

Análisis Económico

- Modelos de precios (on-demand, reservadas, spot)
- Análisis TCO (Total Cost of Ownership)
- Comparativa de costes entre proveedores
- Optimización de gastos

Arquitecturas Cloud Híbridas

Conectividad Híbrida

- VPN y conexiones dedicadas
- Peering de redes
- Gateways de aplicación
- Enrutamiento entre entornos

Gestión de Identidades Híbrida

- Sincronización de directorios

- Autenticación federada
- Single Sign-On (SSO)
- Gestión de accesos unificada

Consistencia de Datos Híbrida

- Replicación de datos entre entornos
- Sincronización de configuraciones
- Resolución de conflictos
- Validación de integridad

Alineación de Soluciones Cloud con Objetivos Empresariales

Traducción de Requisitos de Negocio

- Elicitación de requisitos empresariales
- Mapeo de requisitos a capacidades técnicas
- Definición de criterios de éxito
- Análisis de impacto empresarial

Justificación Económica de Soluciones

- Cálculo de ROI (Return on Investment)
- Análisis de beneficios vs costes
- Período de amortización
- Valor presente neto (NPV)

Comunicación de Decisiones Arquitectónicas

- Presentación a ejecutivos
- Explicación de trade-offs técnicos
- Documentación de decisiones (ADRs)
- Justificación de alternativas rechazadas

Documentación Técnica de Arquitectura

Diagramas Arquitectónicos

- Diagramas de componentes
- Diagramas de flujo de datos
- Diagramas de despliegue
- Vistas de seguridad y cumplimiento

Especificaciones Técnicas

- Descripción de componentes
- Interfaces y contratos de servicios
- Requisitos no funcionales
- Restricciones y limitaciones

Registros de Decisiones Arquitectónicas (ADRs)

- Contexto y problema
- Alternativas evaluadas
- Decisión y justificación
- Consecuencias y trade-offs

Habilidades actitudinales

- Pensamiento sistémico en análisis arquitectónico
- Rigor en evaluación de alternativas
- Comunicación clara de decisiones técnicas a stakeholders
- Orientación a valor empresarial

Justificación

Este bloque agrupa las competencias fundamentales de diseño arquitectónico y evaluación estratégica de soluciones cloud. Las competencias C1, C2, C10 y C20 comparten el propósito común de definir arquitecturas que satisfagan requisitos técnicos y empresariales. La coherencia funcional radica en que todas ellas requieren análisis profundo de alternativas, evaluación de trade-offs y documentación de decisiones. Los entregables compatibles incluyen documentos de arquitectura, matrices de evaluación de proveedores y especificaciones técnicas. Las situaciones de evaluación incluyen diseño de nuevas soluciones, evaluación de proveedores cloud y alineación de requisitos empresariales con especificaciones técnicas.

Ubicación en la progresión

Este bloque constituye la base estratégica y técnica de la formación en cloud computing. Los profesionales comienzan por comprender los patrones arquitectónicos modernos (microservicios, serverless, contenedores) y los principios de escalabilidad y resiliencia. Posteriormente, desarrollan capacidad para evaluar proveedores cloud públicos considerando aspectos técnicos, económicos y de cumplimiento normativo. Finalmente, integran estas habilidades para alinear soluciones cloud con objetivos empresariales, traduciendo requisitos de negocio a especificaciones técnicas. Este bloque habilita el aprendizaje de bloques posteriores de provisión, automatización y operación, ya que establece los fundamentos arquitectónicos sobre los que se construyen las implementaciones.

Bloque 2 - Provisión y Configuración de Infraestructura Cloud

Objetivo pedagógico

Capacitar al profesional para provisionar servicios cloud públicos, configurar controles de seguridad y administrar el ciclo de vida de instancias con hardening y gestión de accesos.

Actividades

Actividad 2.1 Provisionar servicios en plataformas cloud públicas
Actividad 2.2 Desplegar infraestructuras cloud privadas
Actividad 2.3 Configurar entornos cloud híbridos
Actividad 2.4 Diseñar soluciones de red en entornos cloud

Competencias

Competencias	Indicadores
C3 - Provisionar servicios cloud públicos mediante herramientas de Infrastructure as Code garantizando reproducibilidad, versionado y trazabilidad de configuraciones	Código IaC (Terraform, CloudFormation, Pulumi) versionado en repositorio con documentación de cambios Validación de sintaxis y políticas de seguridad en pipelines de despliegue antes de aplicar cambios Auditoría de cambios de infraestructura con trazabilidad completa de quién, qué y cuándo se modificó

Saberes asociados

Herramientas de Infrastructure as Code (IaC)

Terraform

- Sintaxis HCL (HashiCorp Configuration Language)
- Módulos y reutilización de código
- Estados y gestión de estado remoto
- Provisión de recursos en múltiples proveedores cloud
- Validación y planificación de cambios

CloudFormation (AWS)

- Plantillas YAML/JSON
- Stacks y cambios de stack
- Parámetros y salidas
- Políticas de actualización
- Integración con servicios AWS

Pulumi

- Lenguajes de programación (Python, TypeScript, Go)
- Componentes reutilizables
- Gestión de secretos
- Despliegue y actualización de infraestructura

Versionado y control de cambios

- Repositorios Git para código IaC
- Revisión de cambios de infraestructura
- Trazabilidad de configuraciones
- Rollback de cambios

Controles de Seguridad en Cloud

Modelo de responsabilidad compartida

- Responsabilidades del proveedor cloud
- Responsabilidades del cliente
- Diferencias entre IaaS, PaaS y SaaS
- Aplicación en AWS, Azure y GCP

Cifrado de datos

- Cifrado en tránsito (TLS/SSL)
- Cifrado en reposo
- Gestión de claves de cifrado
- Algoritmos de cifrado estándar

Segmentación de red

- Redes virtuales (VPC)
- Subredes públicas y privadas
- Grupos de seguridad y listas de control de acceso (ACLs)
- Aislamiento de tráfico

Estándares de seguridad

- CIS Benchmarks
- ISO 27001
- SOC 2
- NIST Cybersecurity Framework

Gestión de Identidades y Accesos (IAM)

Principio de mínimo privilegio

- Asignación de permisos granulares
- Roles basados en funciones
- Revisión periódica de accesos
- Revocación de accesos innecesarios

Gestión de credenciales

- Autenticación multifactor (MFA)
- Gestión de claves de acceso
- Rotación de credenciales
- Almacenamiento seguro de secretos

Políticas de acceso

- Políticas basadas en identidad
- Políticas basadas en recursos
- Condiciones de acceso
- Auditoría de acceso

Federación de identidades

- Single Sign-On (SSO)
- Integración con directorios corporativos
- Proveedores de identidad externos
- Sincronización de identidades

Hardening y Configuración Segura de Servidores

Configuración base de servidores

- Selección de imágenes base seguras
- Deshabilitación de servicios innecesarios
- Configuración de firewall del sistema operativo
- Aplicación de parches de seguridad

Endurecimiento del sistema operativo

- Configuración de permisos de archivos
- Gestión de usuarios y grupos
- Auditoría y logging
- Configuración de SELinux/AppArmor

Monitoreo de integridad

- Detección de cambios no autorizados
- Verificación de integridad de archivos
- Alertas de cambios de configuración
- Auditoría de cambios

Validación de configuración

- Escaneo de vulnerabilidades
- Evaluación de postura de seguridad
- Cumplimiento de benchmarks
- Documentación de configuración

Provisión de Servicios Cloud Públicos

Servicios de computación

- Instancias de máquinas virtuales (EC2, VMs, Compute Engine)
- Selección de tipos y tamaños de instancias
- Configuración de almacenamiento de instancias
- Gestión del ciclo de vida de instancias

Servicios de red

- Redes virtuales (VPC, VNet, VPC)
- Subredes y enrutamiento
- Balanceadores de carga
- Puertas de enlace NAT y VPN

Servicios de almacenamiento

- Almacenamiento de objetos (S3, Blob Storage, Cloud Storage)
- Almacenamiento en bloque (EBS, Managed Disks, Persistent Disks)
- Almacenamiento de archivos (EFS, Azure Files, Filestore)
- Configuración de acceso y permisos

Servicios de base de datos

- Bases de datos relacionales gestionadas
- Bases de datos NoSQL
- Configuración de copias de seguridad y replicación
- Gestión de acceso a bases de datos

Administración del Ciclo de Vida de Instancias Cloud

Provisión de instancias

- Creación de instancias desde imágenes
- Configuración de parámetros de instancia
- Asignación de recursos (CPU, memoria, almacenamiento)
- Etiquetado y organización de instancias

Gestión de estado

- Estados de instancia (ejecutándose, detenida, terminada)
- Transiciones de estado
- Automatización de cambios de estado
- Recuperación ante fallos

Mantenimiento de instancias

- Aplicación de parches y actualizaciones
- Reinicio y recarga de instancias
- Cambio de tipo de instancia
- Migración de instancias

Desaprovisionamiento

- Terminación de instancias
- Liberación de recursos asociados
- Limpieza de datos residuales
- Auditoría de desaprovisionamiento

Habilidades actitudinales

- Rigor en configuración de seguridad
- Responsabilidad en gestión de accesos
- Atención al detalle en provisión de infraestructura
- Proactividad en identificación de vulnerabilidades

Justificación

Este bloque integra competencias de provisión de infraestructura, configuración de seguridad e identidad. Las competencias C3, C4, C6 y C15 comparten el propósito común de establecer infraestructura cloud segura y bien configurada. La coherencia funcional se basa en que todas requieren conocimiento de herramientas IaC, configuración de controles de seguridad y gestión de accesos. Los entregables compatibles incluyen código IaC versionado, configuraciones de seguridad validadas y políticas IAM granulares. Las situaciones de evaluación incluyen provisión de entornos cloud, implementación de hardening de servidores y configuración de controles de acceso.

Ubicación en la progresión

Este bloque representa la fase de implementación práctica de las arquitecturas diseñadas en el bloque anterior. Los profesionales aprenden a provisionar servicios cloud públicos mediante Infrastructure as Code, garantizando reproducibilidad y trazabilidad. Simultáneamente, desarrollan competencias en configuración de controles de seguridad aplicando el modelo de responsabilidad compartida. Administran el ciclo de vida completo de instancias, desde provisión hasta desaprovisionamiento, aplicando hardening y configuraciones seguras. Implementan gestión de identidades y accesos con principio de mínimo privilegio. Este bloque es esencial para la operación segura de infraestructura cloud y habilita bloques posteriores de automatización, operación y monitoreo.

Bloque 3 - Automatización e Infraestructura como Código

Objetivo pedagógico

Capacitar al profesional para automatizar infraestructura cloud mediante IaC, orquestar contenedores con Kubernetes e implementar soluciones de mensajería asíncrona.

Actividades

Actividad 3.1 Desarrollar scripts y pipelines de automatización de infraestructura
Actividad 3.2 Implementar herramientas de Infrastructure as Code (IaC)
Actividad 3.3 Gestionar configuración y detectar desviaciones (configuration drift)

Competencias

Competencias	Indicadores

Saberes asociados

Herramientas de Infrastructure as Code (IaC)

Terraform

- Sintaxis HCL (HashiCorp Configuration Language)
- Módulos y reutilización de código
- Estado de Terraform y gestión remota
- Provisioners y provisión de recursos
- Validación y planificación de cambios

CloudFormation

- Plantillas YAML/JSON
- Stacks y cambios de stack
- Parámetros y outputs
- Políticas de stack
- Integración con servicios AWS

Pulumi

- Programación en lenguajes generales (Python, Go, TypeScript)
- Stacks y configuración
- Secretos y gestión de credenciales
- Automatización de despliegues
- Integración con CI/CD

Ansible

- Playbooks y roles
- Inventarios y variables
- Módulos de configuración
- Handlers y notificaciones
- Ejecución idempotente

Orquestación de Contenedores con Kubernetes

Conceptos fundamentales de Kubernetes

- Pods y contenedores
- Servicios y exposición de aplicaciones
- Deployments y ReplicaSets
- StatefulSets y DaemonSets
- Namespaces y RBAC

Configuración y gestión de aplicaciones

- ConfigMaps y Secrets
- Volúmenes y almacenamiento persistente
- Probes de salud (liveness, readiness)
- Límites de recursos y requests
- Políticas de escalado automático (HPA)

Despliegue y actualización de aplicaciones

- Estrategias de despliegue (rolling, blue-green, canary)
- Versionado de imágenes de contenedor
- Rollback de despliegues
- Helm para gestión de paquetes
- GitOps y despliegue declarativo

Monitoreo y observabilidad en Kubernetes

- Métricas de Kubernetes (CPU, memoria)
- Logs de contenedores y pods
- Eventos de Kubernetes
- Integración con herramientas de monitoreo
- Alertas basadas en métricas

Arquitecturas de Mensajería y Eventos Asíncronos

Patrones de mensajería asíncrona

- Colas de mensajes (FIFO, estándar)
- Publicador-Suscriptor (Pub/Sub)
- Buses de eventos
- Garantías de entrega (at-least-once, exactly-once)
- Manejo de errores y dead-letter queues

Servicios de mensajería en cloud

- AWS SQS y SNS
- Azure Service Bus y Event Grid
- Google Cloud Pub/Sub
- Apache Kafka en cloud
- RabbitMQ y otros brokers

Diseño de flujos de eventos

- Desacoplamiento de componentes
- Escalabilidad mediante eventos
- Consistencia eventual
- Correlación de eventos
- Trazabilidad de flujos de eventos

Integración de sistemas mediante mensajería

- Adaptadores y transformadores de mensajes
- Enrutamiento de mensajes
- Compensación de transacciones distribuidas
- Monitoreo de flujos de mensajes
- Validación de esquemas de mensajes

Prácticas de Seguridad en Pipelines DevOps

Análisis de vulnerabilidades en código

- SAST (Static Application Security Testing)
- Herramientas de análisis estático (SonarQube, Checkmarx)
- Identificación de patrones de código inseguro
- Gestión de dependencias vulnerables
- Reportes de vulnerabilidades

Análisis dinámico de seguridad

- DAST (Dynamic Application Security Testing)
- Pruebas de penetración automatizadas
- Escaneo de vulnerabilidades en tiempo de ejecución
- Herramientas de DAST (OWASP ZAP, Burp Suite)
- Validación de configuraciones de seguridad

Integración de seguridad en CI/CD

- Gates de seguridad en pipelines
- Automatización de pruebas de seguridad
- Gestión de secretos en pipelines
- Auditoría de cambios de código
- Bloqueo de despliegues inseguros

Gestión de dependencias seguras

- Escaneo de dependencias vulnerables
- Actualización de librerías y frameworks
- Gestión de licencias de software
- Validación de integridad de artefactos
- Repositorios seguros de artefactos

Scripting y Automatización de Infraestructura

Python para automatización

- Scripts de provisión de infraestructura
- Librerías de cloud (boto3, azure-sdk, google-cloud)
- Automatización de tareas operativas
- Procesamiento de datos y logs
- Integración con APIs cloud

Bash y scripting de shell

- Scripts de despliegue
- Automatización de tareas del sistema
- Procesamiento de archivos y logs
- Integración con herramientas CLI
- Manejo de errores y validación

Herramientas de configuración

- Ansible para gestión de configuración
- Chef y Puppet
- Idempotencia en scripts de configuración
- Versionado de configuraciones
- Auditoría de cambios de configuración

Automatización de despliegues

- Scripts de despliegue sin interrupciones
- Rollback automático
- Validación post-despliegue

- Coordinación de despliegues distribuidos
- Monitoreo durante despliegues

Integración de Seguridad en Automatización

Principios de seguridad en IaC

- Gestión de secretos en código IaC
- Validación de configuraciones de seguridad
- Cumplimiento de estándares de seguridad
- Auditoría de cambios de infraestructura
- Trazabilidad de configuraciones

Seguridad en contenedores

- Escaneo de imágenes de contenedor
- Políticas de seguridad de pods
- Gestión de secretos en Kubernetes
- Aislamiento de contenedores
- Cumplimiento de políticas de seguridad

Seguridad en pipelines de automatización

- Autenticación y autorización en pipelines
- Gestión de credenciales en CI/CD
- Auditoría de acciones automatizadas
- Validación de integridad de artefactos
- Prevención de inyección de código

Cumplimiento normativo en automatización

- Trazabilidad de cambios automatizados
- Auditoría de despliegues
- Validación de cumplimiento de políticas
- Documentación de cambios
- Reversibilidad de cambios

Habilidades actitudinales

- Rigor en validación de automatización
- Responsabilidad operativa en automatización
- Pensamiento en seguridad en pipelines
- Orientación a eficiencia operativa

Justificación

Este bloque agrupa competencias de automatización avanzada, orquestación de contenedores e integración asíncrona. Las competencias C7, C9 y C11 comparten el propósito común de automatizar y escalar operaciones cloud. La coherencia funcional radica en que todas requieren conocimiento de herramientas de automatización (Terraform, Kubernetes, servicios de mensajería) y principios de infraestructura declarativa. Los entregables compatibles incluyen manifiestos Kubernetes, código IaC modular y configuraciones de mensajería. Las situaciones de evaluación incluyen despliegue automatizado de aplicaciones, escalado dinámico de contenedores y validación de flujos de mensajería.

Ubicación en la progresión

Este bloque representa la evolución hacia automatización sofisticada de infraestructura y aplicaciones. Los profesionales avanzan desde provisión manual hacia Infrastructure as Code, implementando herramientas

como Terraform para reproducibilidad y versionado. Aprenden a orquestar contenedores con Kubernetes, automatizando despliegue, escalado y gestión del ciclo de vida de aplicaciones. Implementan soluciones de mensajería asíncrona para desacoplamiento de componentes y escalabilidad. Integran análisis de seguridad en pipelines DevOps mediante SAST/DAST. Este bloque habilita operación a escala, permitiendo gestionar infraestructura compleja con mínima intervención manual y es prerequisito para bloques de operación y optimización.

Bloque 4 - Operación, Monitoreo y Optimización de Servicios Cloud

Objetivo pedagógico

Capacitar al profesional para monitorear rendimiento de servicios cloud, optimizar infraestructura y costes, y gestionar operaciones con cumplimiento de SLAs.

Actividades

Actividad 4.1 Configurar herramientas de monitoreo y observabilidad
Actividad 4.2 Definir SLIs, SLOs y analizar tendencias de rendimiento
Actividad 4.3 Gestionar incidentes y resolver problemas operativos
Actividad 4.4 Operar servicios empresariales en la nube

Competencias

Competencias	Indicadores

Saberes asociados

Monitoreo de Rendimiento y Métricas Cloud

Herramientas de Monitoreo APM

- Application Performance Monitoring (APM) en cloud
- Recopilación de métricas de rendimiento
- Trazas distribuidas (distributed tracing)
- Análisis de latencia y throughput
- Herramientas: Datadog, New Relic, Prometheus, CloudWatch

Definición de SLIs y SLOs

- Service Level Indicators (SLIs) cuantificables
- Service Level Objectives (SLOs) alineados con negocio
- Disponibilidad, latencia y tasa de error como SLIs
- Cálculo de error budget
- Comunicación de SLOs a stakeholders

Análisis de Tendencias de Rendimiento

- Análisis histórico de métricas
- Identificación de patrones de carga
- Predicción de tendencias futuras
- Detección de anomalías y desviaciones
- Reportes de tendencias a equipos

Optimización de Costes y Recursos Cloud

Análisis de Utilización de Recursos

- Evaluación de utilización de CPU, memoria y almacenamiento

- Identificación de instancias sobredimensionadas
- Análisis de patrones de uso temporal
- Herramientas de análisis: AWS Compute Optimizer, Azure Advisor
- Benchmarking de rendimiento vs. costes

Estrategias de Compra y Rightsizing

- Instancias reservadas (Reserved Instances)
- Spot instances y precios variables
- Savings Plans y modelos de descuento
- Rightsizing de instancias sin impacto en rendimiento
- Análisis de ROI de cambios de configuración

Gestión de Costes y Reportes

- Desglose de costes por servicio, proyecto y departamento
- Análisis de anomalías de costes
- Presupuestos y alertas de costes
- Reportes de costes a stakeholders
- Identificación de oportunidades de ahorro

Procedimientos Operativos y Gestión de Incidentes

Configuración de Alertas y Dashboards

- Definición de umbrales de alerta basados en SLOs
- Configuración de notificaciones (email, Slack, PagerDuty)
- Creación de dashboards operativos personalizados
- Visualización de métricas críticas en tiempo real
- Escalado automático de alertas según severidad

Respuesta a Incidentes y Troubleshooting

- Procedimientos de respuesta a incidentes (runbooks)
- Investigación de causas raíz de problemas
- Escalado de incidentes a equipos especializados
- Comunicación de estado durante incidentes
- Post-mortem y lecciones aprendidas

Mantenimiento Preventivo y Optimización

- Revisiones periódicas de configuración
- Aplicación de parches y actualizaciones
- Limpieza de recursos no utilizados
- Validación de cumplimiento de SLAs
- Mejora continua de procesos operativos

Plataformas Cloud Públicas y Servicios Gestionados

Servicios de Monitoreo en Proveedores Cloud

- AWS CloudWatch, CloudTrail y X-Ray
- Azure Monitor, Application Insights y Log Analytics
- Google Cloud Monitoring, Logging y Trace
- Integración de servicios de monitoreo nativos
- Exportación de métricas a herramientas externas

Servicios de Optimización en Proveedores Cloud

- AWS Cost Explorer, Compute Optimizer y Trusted Advisor
- Azure Cost Management y Advisor
- Google Cloud Cost Management Tools
- Recomendaciones automáticas de optimización
- Integración con herramientas de FinOps

Configuración de Escalado Automático

- Auto Scaling Groups en AWS
- Virtual Machine Scale Sets en Azure
- Instance Groups en Google Cloud
- Políticas de escalado basadas en métricas
- Validación de escalado sin impacto en usuarios

Herramientas de Monitoreo y Observabilidad

Herramientas de Observabilidad Integral

- Stack de observabilidad: métricas, logs y trazas
- Prometheus para recopilación de métricas
- ELK Stack (Elasticsearch, Logstash, Kibana) para logs
- Jaeger y Zipkin para trazas distribuidas
- Integración de múltiples fuentes de datos

Análisis de Datos de Monitoreo

- Consultas avanzadas en herramientas de monitoreo
- Correlación de eventos entre múltiples fuentes
- Análisis de patrones y anomalías
- Machine Learning para detección de anomalías
- Visualización de datos complejos

Automatización de Respuestas Operativas

- Webhooks y integraciones con sistemas externos
- Automatización de acciones correctivas
- Orquestación de respuestas a incidentes
- Integración con herramientas de ticketing
- Auditoría de acciones automatizadas

Gestión de Acuerdos de Nivel de Servicio (SLA)

Definición y Comunicación de SLAs

- Componentes de un SLA (disponibilidad, latencia, throughput)
- Cálculo de error budget y tolerancia de fallos
- Comunicación clara de SLAs a stakeholders
- Documentación de compromisos de servicio
- Revisión periódica de SLAs con negocio

Monitoreo de Cumplimiento de SLAs

- Cálculo automático de cumplimiento de SLAs
- Alertas cuando SLA está en riesgo
- Reportes de cumplimiento a stakeholders
- Análisis de causas de incumplimiento
- Acciones correctivas para recuperar SLA

Mejora Continua de Disponibilidad

- Análisis de incidentes que afectaron SLA
- Implementación de mejoras de resiliencia
- Validación de mejoras mediante simulacros
- Documentación de lecciones aprendidas
- Comunicación de mejoras a stakeholders

Habilidades actitudinales

- Proactividad en detección de problemas

- Disciplina en cumplimiento de SLAs
- Orientación a optimización de costes
- Comunicación clara de estado operativo

Justificación

Este bloque integra competencias de monitoreo, optimización y gestión operativa. Las competencias C5, C16, C21, C22 y C25 comparten el propósito común de garantizar operación eficiente y económica de servicios cloud. La coherencia funcional se basa en que todas requieren conocimiento de herramientas de monitoreo, análisis de métricas y optimización de recursos. Los entregables compatibles incluyen dashboards de monitoreo, reportes de costes y procedimientos operativos estándar. Las situaciones de evaluación incluyen configuración de alertas, análisis de tendencias de rendimiento, rightsizing de instancias y reportes de SLA.

Ubicación en la progresión

Este bloque representa la fase de operación sostenible y optimización continua de infraestructura cloud. Los profesionales aprenden a monitorear rendimiento mediante métricas, trazas distribuidas y análisis de tendencias, estableciendo dashboards alineados con SLIs y SLOs. Desarrollan capacidad para identificar oportunidades de optimización mediante análisis de utilización de recursos y implementan estrategias de rightsizing. Gestionan operaciones mediante procedimientos estándar (SOPs) y aseguran cumplimiento de SLAs. Analizan costes detalladamente, identifican anomalías y recomiendan estrategias de compra (instancias reservadas, spot). Este bloque es esencial para operación a largo plazo y habilita toma de decisiones informada sobre infraestructura.

Bloque 5 - Gestión de Servidores, Software y Contenedores

Objetivo pedagógico

Capacitar al profesional para administrar ciclo de vida de instancias cloud, orquestar contenedores y gestionar software en entornos cloud.

Actividades

Actividad 5.1 Administrar instancias de cómputo cloud
Actividad 5.2 Gestionar el ciclo de vida de aplicaciones y servicios software
Actividad 5.3 Administrar plataformas de orquestación de contenedores

Competencias

Competencias	Indicadores
C6 - Administrar ciclo de vida de instancias cloud aplicando hardening y configuración segura para garantizar disponibilidad y seguridad operativa	Implementación de imágenes base endurecidas (golden images) con parches de seguridad y configuraciones CIS Automatización de aprovisionamiento, escalado y desaprovisionamiento de instancias según políticas definidas Monitoreo continuo de estado, rendimiento y cumplimiento de configuración de servidores en producción
C7 - Orquestar contenedores en plataformas cloud utilizando Kubernetes para automatizar despliegue, escalado y gestión del ciclo de vida de aplicaciones	Definición de manifiestos Kubernetes (Deployments, Services, ConfigMaps, Secrets) con buenas prácticas de seguridad Configuración de políticas de escalado automático (HPA) basadas en métricas de CPU, memoria o métricas personalizadas Implementación de estrategias de actualización (rolling updates, blue-green) con validación de salud y rollback automático

Saberes asociados

Administración del Ciclo de Vida de Instancias Cloud

Provisión de instancias cloud

- Creación de instancias en AWS EC2, Azure VMs, GCP Compute Engine
- Configuración de tipos de instancia y tamaños
- Asignación de almacenamiento y redes
- Automatización de provisión mediante IaC

Configuración segura de servidores

- Hardening de sistemas operativos (Linux, Windows)
- Aplicación de parches de seguridad
- Deshabilitación de servicios innecesarios
- Configuración de firewalls y grupos de seguridad

Monitoreo de estado y rendimiento

- Recopilación de métricas de CPU, memoria y disco
- Configuración de alertas de disponibilidad
- Análisis de logs de sistema

- Detección de anomalías de rendimiento

Desaprovisionamiento y limpieza

- Procedimientos de terminación segura de instancias
- Eliminación de volúmenes y snapshots
- Auditoría de recursos huérfanos
- Automatización de limpieza de recursos

Orquestación de Contenedores con Kubernetes

Conceptos fundamentales de Kubernetes

- Pods, Deployments, Services y ConfigMaps
- Namespaces y RBAC (Role-Based Access Control)
- Persistent Volumes y almacenamiento
- Ingress y gestión de tráfico

Despliegue de aplicaciones en Kubernetes

- Creación de manifiestos YAML
- Estrategias de despliegue (rolling, blue-green, canary)
- Gestión de versiones de imágenes
- Automatización de despliegues con CI/CD

Escalado automático de aplicaciones

- Horizontal Pod Autoscaler (HPA)
- Vertical Pod Autoscaler (VPA)
- Cluster Autoscaler
- Políticas de escalado basadas en métricas personalizadas

Gestión del ciclo de vida de contenedores

- Actualización de imágenes de contenedores
- Rollback de despliegues
- Limpieza de imágenes obsoletas
- Monitoreo de salud de contenedores (liveness y readiness probes)

Gestión del Software en Entornos Cloud

Herramientas de gestión de configuración

- Ansible: playbooks, roles y módulos
- Chef: recetas, cookbooks y atributos
- Puppet: manifiestos y módulos
- Comparativa y selección de herramientas

Gestión del ciclo de vida de aplicaciones

- Despliegue de aplicaciones en instancias cloud
- Actualización y parches de aplicaciones
- Gestión de dependencias de software
- Automatización de instalación y configuración

Orquestación de servicios

- Coordinación de múltiples componentes de aplicación
- Gestión de dependencias entre servicios
- Automatización de flujos de despliegue complejos
- Validación de integridad post-despliegue

Monitoreo de aplicaciones

- Recopilación de logs de aplicación
- Métricas de rendimiento de aplicación (APM)
- Alertas basadas en comportamiento de aplicación

- Análisis de trazas distribuidas

Arquitecturas Asíncronas y Mensajería

Patrones de mensajería asíncrona

- Colas de mensajes (SQS, Service Bus, RabbitMQ)
- Publicación-Suscripción (SNS, Event Grid, Pub/Sub)
- Buses de eventos (Kafka, Event Hubs)
- Garantías de entrega y procesamiento

Desacoplamiento de componentes

- Comunicación asíncrona entre servicios
- Reducción de dependencias directas
- Mejora de escalabilidad y resiliencia
- Manejo de fallos en sistemas distribuidos

Configuración de servicios de mensajería

- Creación de colas y tópicos
- Configuración de políticas de retención
- Gestión de dead-letter queues
- Monitoreo de flujos de mensajes

Patrones de consumo de mensajes

- Procesamiento de mensajes en lotes
- Manejo de errores y reintentos
- Idempotencia en procesamiento
- Validación de integridad de mensajes

Herramientas de Automatización e IaC

Infrastructure as Code (IaC)

- Terraform: módulos, variables y outputs
- CloudFormation: templates y stacks
- Pulumi: infraestructura como código en lenguajes de programación
- Versionado y gestión de cambios de infraestructura

Scripting y automatización

- Python para automatización de tareas cloud
- Bash para scripting en Linux
- Ansible para automatización de configuración
- Integración de scripts en pipelines CI/CD

Gestión de estado de infraestructura

- Archivos de estado en Terraform
- Sincronización de estado entre equipos
- Recuperación ante fallos de estado
- Auditoría de cambios de infraestructura

Validación y pruebas de automatización

- Validación de sintaxis de IaC
- Pruebas de configuración antes de despliegue
- Simulación de cambios (plan vs apply)
- Rollback automático ante fallos

Seguridad en Gestión de Componentes Cloud

Hardening de instancias y contenedores

- Configuración de grupos de seguridad y firewalls

- Gestión de claves SSH y credenciales
- Aplicación de políticas de contraseñas
- Deshabilitación de protocolos inseguros

Gestión de identidades en componentes

- Roles IAM para instancias y contenedores
- Principio de mínimo privilegio en permisos
- Auditoría de accesos a componentes
- Rotación de credenciales

Seguridad de imágenes de contenedores

- Escaneo de vulnerabilidades en imágenes
- Firma digital de imágenes
- Registros de contenedores seguros
- Políticas de admisión en Kubernetes

Monitoreo de seguridad de componentes

- Detección de cambios no autorizados
- Análisis de logs de auditoría
- Alertas de acceso sospechoso
- Validación de integridad de configuraciones

Habilidades actitudinales

- Atención al detalle en configuración de componentes
- Responsabilidad en mantenimiento de componentes
- Orientación a automatización de tareas repetitivas
- Capacidad de diagnóstico de problemas

Justificación

Este bloque agrupa competencias de administración de servidores, orquestación de contenedores y gestión de software. Las competencias C6, C7 y C11 comparten el propósito común de gestionar componentes de infraestructura y aplicaciones. La coherencia funcional radica en que todas requieren conocimiento de herramientas de gestión (Kubernetes, Ansible, herramientas de configuración) y principios de automatización. Los entregables compatibles incluyen manifiestos Kubernetes, playbooks de Ansible y políticas de escalado. Las situaciones de evaluación incluyen provisión de instancias, despliegue de contenedores y escalado automático de aplicaciones.

Ubicación en la progresión

Este bloque representa la gestión integral de componentes de infraestructura y aplicaciones en cloud. Los profesionales administran ciclo de vida completo de instancias, desde provisión hasta desaprovisionamiento, aplicando hardening y configuraciones seguras. Orquestan contenedores con Kubernetes, automatizando despliegue, escalado y gestión del ciclo de vida. Gestionan software mediante herramientas de configuración (Ansible, Chef, Puppet) y Kubernetes. Implementan estrategias de escalado automático basadas en métricas. Este bloque integra conocimientos de provisión, automatización y operación para proporcionar visión holística de gestión de componentes cloud.

Bloque 6 - Integración de Sistemas y Arquitecturas de Mensajería

Objetivo pedagógico

Capacitar al profesional para integrar soluciones cloud con sistemas heredados mediante APIs y mensajería, coordinando proyectos de integración.

Actividades

Actividad 6.1 Integrar servicios cloud con sistemas existentes
Actividad 6.2 Implementar soluciones de mensajería y eventos en cloud

Competencias

Competencias	Indicadores
C8 - Integrar soluciones cloud con sistemas heredados mediante APIs, colas de mensajes y buses de eventos para garantizar interoperabilidad y consistencia de datos	Diseño de patrones de integración (síncrono con APIs, asíncrono con colas/eventos) documentados con diagramas de flujo Implementación de adaptadores y transformadores de datos para compatibilidad entre sistemas heterogéneos Validación de integridad de datos y manejo de errores en escenarios de fallo de conectividad o latencia
C11 - Implementar soluciones de mensajería y eventos en cloud diseñando arquitecturas asíncronas para desacoplamiento de componentes y escalabilidad	Selección y configuración de servicios de mensajería (SQS/SNS, Service Bus, Pub/Sub, Kafka) según patrones de comunicación Implementación de mecanismos de reintentos, dead-letter queues y manejo de errores en flujos asíncronos Validación de entrega de mensajes, orden de procesamiento y idempotencia en consumidores

Saberes asociados

Patrones de Integración de Sistemas

Patrones de integración síncrona

- APIs REST y SOAP
- Llamadas síncronas punto a punto
- Gestión de timeouts y reintentos
- Versionado de APIs

Patrones de integración asíncrona

- Colas de mensajes (SQS, Service Bus, RabbitMQ)
- Buses de eventos (Event Hub, Kafka, Pub/Sub)
- Publicador-Suscriptor
- Garantías de entrega (at-least-once, exactly-once)

Transformación de datos en integraciones

- Mapeo de esquemas entre sistemas
- Transformación de formatos (JSON, XML, Protobuf)
- Validación de datos en flujos de integración

- Manejo de incompatibilidades de datos

Arquitecturas de Mensajería en Cloud

Servicios de mensajería cloud

- Amazon SQS y SNS
- Azure Service Bus y Event Hub
- Google Cloud Pub/Sub
- Apache Kafka en cloud
- Características de cada servicio (latencia, throughput, durabilidad)

Diseño de arquitecturas asíncronas

- Desacoplamiento de componentes
- Escalabilidad mediante mensajería
- Manejo de errores y dead letter queues
- Idempotencia en procesamiento de mensajes
- Ordenamiento de mensajes

Patrones de eventos

- Event sourcing
- CQRS (Command Query Responsibility Segregation)
- Saga distribuida para transacciones
- Event streaming

Integración de Sistemas Heredados

Análisis de sistemas heredados

- Identificación de dependencias y acoplamiento
- Evaluación de compatibilidad con cloud
- Documentación de interfaces existentes
- Análisis de limitaciones técnicas

Estrategias de integración con legados

- Adaptadores y conectores
- Puentes de integración (integration bridges)
- Migración gradual de funcionalidad
- Mantenimiento de compatibilidad hacia atrás

Protocolos y estándares de integración

- HTTP/HTTPS y REST
- SOAP y Web Services
- EDI (Electronic Data Interchange)
- FTP y SFTP para transferencia de archivos
- Protocolos propietarios

Consistencia de Datos en Integraciones

Garantías de consistencia

- Consistencia eventual
- Transacciones distribuidas
- Compensación de transacciones
- Reconciliación de datos

Validación de integridad de datos

- Checksums y hashes
- Validación de esquema
- Detección de duplicados
- Auditoría de cambios de datos

Manejo de errores en flujos de integración

- Reintentos con backoff exponencial
- Circuit breaker pattern
- Dead letter queues
- Logging y trazabilidad de errores

Coordinación de Proyectos de Integración

Planificación de proyectos de integración

- Análisis de requisitos de integración
- Estimación de esfuerzo y cronograma
- Identificación de riesgos de integración
- Definición de criterios de éxito

Gestión de equipos en integraciones

- Coordinación entre equipos de sistemas heredados y cloud
- Comunicación de cambios y dependencias
- Resolución de conflictos técnicos
- Seguimiento de desviaciones de proyecto

Validación y pruebas de integraciones

- Pruebas de integración end-to-end
- Pruebas de carga y rendimiento
- Pruebas de recuperación ante fallos
- Validación en entornos de staging

Documentación de Flujos de Integración

Documentación técnica de integraciones

- Diagramas de flujo de datos
- Especificación de contratos de API
- Documentación de esquemas de mensajes
- Mapeo de transformaciones de datos

Procedimientos operativos de integración

- Runbooks de despliegue de integraciones
- Procedimientos de monitoreo de flujos
- Procedimientos de recuperación ante fallos
- Procedimientos de mantenimiento

Comunicación de decisiones de integración

- Justificación de patrones seleccionados
- Documentación de trade-offs
- Explicación de limitaciones conocidas
- Recomendaciones para evolución futura

Habilidades actitudinales

- Comprensión profunda de sistemas heterogéneos
- Rigor en validación de integraciones
- Comunicación clara entre equipos técnicos
- Orientación a confiabilidad de integraciones

Justificación

Este bloque agrupa competencias de integración de sistemas, arquitecturas de mensajería y coordinación de proyectos. Las competencias C8, C11 y C18 comparten el propósito común de conectar sistemas heterogéneos y garantizar interoperabilidad. La coherencia funcional se basa en que todas requieren conocimiento de patrones de integración (síncrono y asíncrono), servicios de mensajería y gestión de proyectos. Los entregables compatibles incluyen diagramas de flujo de integración, configuraciones de colas de mensajes y planes de proyecto. Las situaciones de evaluación incluyen diseño de integraciones, implementación de flujos de mensajería y coordinación de equipos de integración.

Ubicación en la progresión

Este bloque representa la integración de soluciones cloud con ecosistemas empresariales existentes. Los profesionales diseñan patrones de integración (síncronos con APIs, asíncronos con colas/eventos) documentados con claridad. Implementan adaptadores y transformadores de datos para compatibilidad entre sistemas heterogéneos. Configuran servicios de mensajería cloud (SQS/SNS, Service Bus, Pub/Sub, Kafka) con garantías de entrega y manejo de errores. Coordinan proyectos de integración gestionando cronograma, recursos y riesgos. Este bloque habilita modernización de sistemas heredados mediante integración con servicios cloud.

Bloque 7 - Seguridad Cloud y Cumplimiento Normativo

Objetivo pedagógico

Capacitar al profesional para garantizar seguridad de servicios cloud, aplicar controles de seguridad, gestionar identidades y promover cultura de seguridad.

Actividades

Actividad 7.1 Aplicar buenas prácticas de desarrollo seguro en cloud
Actividad 7.2 Definir e implementar controles de seguridad cloud
Actividad 7.3 Administrar identidades y accesos en la nube
Actividad 7.4 Identificar y mitigar vulnerabilidades de seguridad
Actividad 7.5 Asegurar cumplimiento normativo y promover cultura de seguridad

Competencias

Competencias	Indicadores
C4 - Configurar controles de seguridad en entornos cloud aplicando modelo de responsabilidad compartida para proteger datos y servicios contra amenazas	Implementación de cifrado en tránsito y en reposo con gestión centralizada de claves (KMS) Configuración de grupos de seguridad, listas de control de acceso (ACLs) y segmentación de redes virtuales Validación de postura de seguridad mediante herramientas de evaluación (CIS Benchmarks, AWS Config, Azure Policy)
C9 - Aplicar prácticas de desarrollo seguro integrando análisis de vulnerabilidades en pipelines DevOps para identificar y mitigar riesgos de seguridad tempranamente	Integración de herramientas SAST (análisis estático) y DAST (análisis dinámico) en fases de build y test del pipeline Gestión automatizada de dependencias con detección de vulnerabilidades conocidas (CVEs) y actualización de librerías Revisión de código enfocada en patrones de seguridad (inyecciones, exposición de credenciales, validación de entrada)
C15 - Administrar identidades y accesos en cloud aplicando principio de mínimo privilegio para controlar autorización y auditar acceso a recursos	Configuración de políticas IAM granulares con roles basados en responsabilidades y principio de mínimo privilegio Implementación de autenticación multifactor (MFA) y acceso condicional basado en contexto (ubicación, dispositivo, riesgo) Auditoría de accesos con logs de CloudTrail/Activity Log y revisión periódica de permisos asignados

Saberes asociados

Seguridad en Entornos Cloud

Modelo de Responsabilidad Compartida

- Responsabilidades del proveedor cloud
- Responsabilidades del cliente
- Diferencias entre modelos IaaS, PaaS, SaaS
- Evaluación de responsabilidades por servicio

Controles de Seguridad en Cloud

- Cifrado en tránsito y en reposo
- Gestión de claves criptográficas
- Segmentación de redes virtuales
- Firewalls y grupos de seguridad
- Detección y prevención de intrusiones

Estándares y Marcos de Seguridad

- ISO 27001 y familia ISO 27000
- CIS Benchmarks para cloud
- AWS Well-Architected Framework (pilar seguridad)
- Azure Security Benchmark
- NIST Cybersecurity Framework

Gestión de Identidades y Accesos (IAM)

Principios de Control de Acceso

- Principio de mínimo privilegio
- Separación de funciones
- Control de acceso basado en roles (RBAC)
- Control de acceso basado en atributos (ABAC)
- Revisión periódica de accesos

Autenticación y Autorización

- Autenticación multifactor (MFA)
- Gestión de credenciales
- Federación de identidades
- Single Sign-On (SSO)
- Políticas de contraseñas

Auditoría y Cumplimiento de Accesos

- Logging de accesos y eventos
- Análisis de logs de auditoría
- Detección de accesos anómalos
- Reportes de cumplimiento de accesos
- Investigación de incidentes de seguridad

Cumplimiento Normativo en Cloud

Regulaciones y Normativas Aplicables

- RGPD (Reglamento General de Protección de Datos)
- LOPD-GDD (Ley Orgánica de Protección de Datos)
- SOC 2 (Service Organization Control)
- PCI-DSS (Payment Card Industry Data Security Standard)
- HIPAA (Health Insurance Portability and Accountability Act)
- Normativas sectoriales específicas

Evaluación de Cumplimiento

- Auditorías de cumplimiento
- Evaluaciones de conformidad
- Certificaciones de seguridad
- Informes de cumplimiento
- Mapeo de requisitos normativos

Residencia y Soberanía de Datos

- Requisitos de localización de datos
- Restricciones de transferencia internacional
- Cumplimiento de soberanía de datos

- Selección de regiones cloud
- Documentación de ubicación de datos

Análisis de Vulnerabilidades y Pruebas de Seguridad

Pruebas de Seguridad Estáticas y Dinámicas

- SAST (Static Application Security Testing)
- DAST (Dynamic Application Security Testing)
- Análisis de dependencias
- Escaneo de vulnerabilidades de contenedores
- Pruebas de penetración

Integración de Seguridad en Pipelines

- DevSecOps y automatización de seguridad
- Escaneo de código en CI/CD
- Validación de artefactos
- Políticas de seguridad en despliegue
- Bloqueo de despliegues inseguros

Gestión de Vulnerabilidades

- Identificación de vulnerabilidades
- Evaluación de severidad
- Priorización de remediación
- Seguimiento de parches
- Validación de correcciones

Cultura y Prácticas de Seguridad

Promoción de Cultura de Seguridad

- Liderazgo en seguridad
- Formación y concienciación en seguridad
- Comunicación de riesgos de seguridad
- Ejemplificación de comportamientos seguros
- Influencia positiva en adopción de controles

Vigilancia y Respuesta a Incidentes

- Monitoreo activo de eventos de seguridad
- Investigación de alertas de seguridad
- Respuesta inmediata a incidentes
- Documentación de incidentes
- Análisis post-incidente

Responsabilidad en Aplicación de Controles

- Aplicación consistente de estándares
- Revocación inmediata de accesos
- Documentación de cambios de seguridad
- Validación de cumplimiento
- Mejora continua de controles

Herramientas y Servicios de Seguridad Cloud

Servicios de Seguridad en Proveedores Cloud

- AWS Security Hub, GuardDuty, Inspector
- Azure Security Center, Defender, Sentinel
- GCP Security Command Center, Cloud Armor
- Servicios de gestión de secretos
- Servicios de encriptación gestionados

Herramientas de Evaluación y Monitoreo

- Herramientas de escaneo de configuración
- Herramientas de análisis de postura de seguridad
- SIEM (Security Information and Event Management)
- Herramientas de detección de anomalías
- Dashboards de seguridad

Automatización de Controles de Seguridad

- Políticas de seguridad automatizadas
- Remediación automática de desviaciones
- Orquestación de respuesta a incidentes
- Automatización de auditoría
- Reportes automatizados de cumplimiento

Habilidades actitudinales

- Vigilancia continua de seguridad
- Responsabilidad en aplicación de controles
- Comunicación clara de riesgos de seguridad
- Liderazgo en cultura de seguridad

Justificación

Este bloque integra competencias de seguridad cloud, cumplimiento normativo y promoción de cultura de seguridad. Las competencias C4, C9, C15, C23, C24 y C39 comparten el propósito común de proteger servicios cloud contra amenazas. La coherencia funcional se basa en que todas requieren conocimiento de estándares de seguridad (ISO 27001, SOC 2, CIS Benchmarks), controles técnicos y gestión de identidades. Los entregables compatibles incluyen políticas de seguridad, configuraciones de controles y programas de formación. Las situaciones de evaluación incluyen evaluación de postura de seguridad, implementación de controles y formación de equipos.

Ubicación en la progresión

Este bloque representa el pilar de seguridad en operación de servicios cloud. Los profesionales comprenden el modelo de responsabilidad compartida y aplican controles de seguridad en todos los niveles. Implementan cifrado en tránsito y en reposo, configuran gestión de identidades y accesos con principio de mínimo privilegio, y segmentan redes virtuales. Integran análisis de vulnerabilidades en pipelines DevOps mediante SAST/DAST. Evalúan postura de seguridad contra estándares (CIS Benchmarks, AWS Config, Azure Policy). Promueven cultura de seguridad mediante formación y elaboración de guías. Este bloque es transversal a todos los aspectos de operación cloud y es crítico para cumplimiento normativo.

Bloque 8 - Almacenamiento, Datos y Bases de Datos Cloud

Objetivo pedagógico

Capacitar al profesional para diseñar soluciones de almacenamiento cloud, migrar datos y gestionar bases de datos gestionadas.

Actividades

Actividad 8.1 Diseñar soluciones de almacenamiento cloud
Actividad 8.2 Administrar bases de datos en la nube
Actividad 8.3 Migrar datos a la nube

Competencias

Competencias	Indicadores
C1 - Diseñar arquitecturas cloud escalables y resilientes aplicando patrones arquitectónicos modernos para satisfacer requisitos de disponibilidad y rendimiento	Documentación de arquitectura que incluye patrones de microservicios, serverless o contenedores con justificación técnica Evaluación de escalabilidad horizontal y vertical con métricas de capacidad y crecimiento proyectado Validación de resiliencia mediante análisis de puntos de fallo único y estrategias de redundancia
C13 - Migrar datos a cloud garantizando integridad, seguridad y validación mediante procesos automatizados y reconciliación de datos	Selección de herramientas de migración de datos (AWS DMS, Azure Data Factory, Google Cloud Transfer) según volumen y tipo Implementación de validaciones de integridad (checksums, row counts, muestreo de datos) antes y después de migración Documentación de mapeo de datos, transformaciones aplicadas y procedimientos de rollback en caso de inconsistencias

Saberes asociados

Almacenamiento en la Nube

Tipos de almacenamiento cloud

- Almacenamiento de objetos (S3, Azure Blob Storage, Google Cloud Storage)
- Almacenamiento en bloque (EBS, Azure Managed Disks, Persistent Disks)
- Almacenamiento de archivos (EFS, Azure Files, Filestore)
- Almacenamiento de datos fríos y archivos (Glacier, Archive Storage)

Configuración y gestión de almacenamiento

- Políticas de ciclo de vida de datos
- Versionado de objetos
- Replicación y redundancia
- Cifrado en reposo y en tránsito
- Control de acceso a almacenamiento

Optimización de costes de almacenamiento

- Selección de clases de almacenamiento económicas
- Compresión y deduplicación de datos

- Análisis de utilización de almacenamiento
- Estrategias de retención de datos

Migración de Datos a Cloud

Estrategias de migración de datos

- Migración por lotes (batch migration)
- Migración incremental (incremental migration)
- Migración en tiempo real (live migration)
- Herramientas de migración (AWS DataSync, Azure Data Box, Google Transfer Service)

Validación e integridad de datos

- Reconciliación de datos post-migración
- Validación de checksums y hashes
- Pruebas de integridad referencial
- Auditoría de migración de datos

Seguridad en migración de datos

- Cifrado durante la transferencia
- Cumplimiento de regulaciones (GDPR, HIPAA)
- Gestión de datos sensibles
- Eliminación segura de datos origen

Bases de Datos Gestionadas en Cloud

Tipos de bases de datos cloud

- Bases de datos relacionales gestionadas (RDS, Azure SQL, Cloud SQL)
- Bases de datos NoSQL (DynamoDB, Cosmos DB, Firestore)
- Bases de datos de series temporales (TimescaleDB, InfluxDB)
- Almacenes de datos (Redshift, BigQuery, Synapse Analytics)

Configuración y administración de bases de datos

- Provisión de instancias de base de datos
- Configuración de réplicas y alta disponibilidad
- Backup y restauración automatizados
- Escalado automático de capacidad
- Monitoreo de rendimiento de bases de datos

Optimización de bases de datos

- Indexación y optimización de consultas
- Particionamiento de datos
- Caché distribuido (Redis, Memcached)
- Análisis de costes de bases de datos

Arquitectura de Datos en Cloud

Patrones de arquitectura de datos

- Data Lake (lago de datos)
- Data Warehouse (almacén de datos)
- Arquitectura lambda (batch + streaming)
- Arquitectura kappa (streaming)
- Arquitectura medallion (bronze, silver, gold)

Integración de datos

- ETL (Extract, Transform, Load)
- ELT (Extract, Load, Transform)
- Pipelines de datos
- Sincronización de datos en tiempo real

Gobernanza de datos

- Catálogo de datos
- Linaje de datos
- Calidad de datos
- Metadatos y documentación

Seguridad y Cumplimiento en Almacenamiento de Datos

Protección de datos

- Cifrado de datos en reposo
- Cifrado de datos en tránsito
- Gestión de claves de cifrado (KMS)
- Enmascaramiento de datos sensibles

Control de acceso a datos

- Políticas de acceso granulares
- Autenticación y autorización
- Auditoría de acceso a datos
- Principio de mínimo privilegio

Cumplimiento normativo

- GDPR y privacidad de datos
- HIPAA para datos de salud
- PCI-DSS para datos de pago
- Residencia de datos y soberanía

Herramientas y Servicios de Gestión de Datos Cloud

Herramientas de migración y sincronización

- AWS DataSync, AWS DMS, AWS Snowball
- Azure Data Factory, Azure Data Box
- Google Cloud Data Transfer Service
- Herramientas de código abierto (Kafka, Airflow)

Herramientas de monitoreo y análisis

- CloudWatch, Azure Monitor, Cloud Monitoring
- Herramientas de análisis de costes
- Dashboards de rendimiento de datos
- Alertas y notificaciones

Herramientas de gobernanza y calidad

- Catálogos de datos (Glue, Purview, Data Catalog)
- Herramientas de calidad de datos
- Herramientas de linaje de datos
- Soluciones de cumplimiento normativo

Habilidades actitudinales

- Rigor en validación de integridad de datos
- Orientación a optimización de costes de almacenamiento
- Responsabilidad en seguridad de datos
- Atención al detalle en configuración de almacenamiento

Justificación

Este bloque agrupa competencias de diseño de almacenamiento, migración de datos y gestión de bases de datos. Las competencias C1, C13 y C31 comparten el propósito común de gestionar datos en cloud de forma segura y eficiente. La coherencia funcional se basa en que todas requieren conocimiento de tipos de almacenamiento (objeto, bloque, archivo), bases de datos gestionadas y políticas de ciclo de vida. Los entregables compatibles incluyen diseños de soluciones de almacenamiento, planes de migración de datos y políticas de retención. Las situaciones de evaluación incluyen selección de tipos de almacenamiento, migración de datos y configuración de políticas de ciclo de vida.

Ubicación en la progresión

Este bloque representa la gestión integral de datos en cloud. Los profesionales diseñan soluciones de almacenamiento seleccionando tipos apropiados (objeto, bloque, archivo) según requisitos de acceso y rendimiento. Migran datos a cloud garantizando integridad mediante validaciones y reconciliación. Implementan políticas de ciclo de vida de datos para optimizar costes. Diseñan arquitecturas de bases de datos gestionadas aprovechando servicios cloud. Este bloque es esencial para modernización de sistemas de datos y habilita análisis y procesamiento de datos en cloud.

Bloque 9 - Continuidad, Recuperación y Copias de Seguridad

Objetivo pedagógico

Capacitar al profesional para diseñar planes de continuidad de negocio, implementar copias de seguridad y restaurar servicios ante incidentes.

Actividades

Actividad 9.1 Diseñar planes de continuidad y recuperación ante desastres
Actividad 9.2 Implementar políticas y procedimientos de backup
Actividad 9.3 Restaurar servicios tras incidentes cloud

Competencias

Competencias	Indicadores
C14 - Diseñar e implementar planes de continuidad de negocio y recuperación ante desastres definiendo RTO y RPO para garantizar resiliencia operativa	Documentación de planes BCP/DRP con definición clara de RTO (Objetivo de Tiempo de Recuperación) y RPO (Objetivo de Punto de Recuperación) Implementación de estrategias de backup automatizado con validación periódica de restauración en entornos de prueba Ejecución de simulacros de recuperación ante desastres con registro de resultados y lecciones aprendidas

Saberes asociados

Planes de Continuidad de Negocio y Recuperación ante Desastres

Conceptos fundamentales de continuidad

- Definición de BCP (Plan de Continuidad de Negocio)
- Definición de DRP (Plan de Recuperación ante Desastres)
- Diferencias entre BCP y DRP
- Marcos de referencia (ISO 22301, NIST)
- Análisis de impacto empresarial (BIA)

Definición de objetivos de recuperación

- RTO (Recovery Time Objective) - Tiempo máximo de recuperación
- RPO (Recovery Point Objective) - Punto máximo de pérdida de datos
- Cálculo de RTO y RPO según criticidad de servicios
- Alineación de RTO/RPO con requisitos empresariales
- Documentación de objetivos de recuperación

Estrategias de recuperación

- Recuperación en sitio alterno (hot site, warm site, cold site)
- Replicación de datos en tiempo real
- Failover automático y manual
- Estrategias de recuperación por capas (infraestructura, datos, aplicaciones)
- Planes de escalada y comunicación durante desastres

Estrategias y Tecnologías de Copias de Seguridad

Tipos de copias de seguridad

- Copias completas (full backup)
- Copias incrementales (incremental backup)
- Copias diferenciales (differential backup)
- Copias de espejo (mirror backup)
- Copias continuas (continuous data protection)

Políticas de retención y ciclo de vida

- Definición de políticas de retención según regulación
- Ciclo de vida de datos (hot, warm, cold storage)
- Automatización de políticas de retención
- Cumplimiento normativo en retención de datos
- Gestión de almacenamiento de backups

Validación y restauración de backups

- Pruebas de restauración (restore testing)
- Validación de integridad de backups
- Procedimientos de restauración granular
- Recuperación de datos específicos
- Documentación de procedimientos de restauración

Servicios de Copias de Seguridad en Cloud

Servicios de backup nativos de proveedores cloud

- AWS Backup, AWS S3 Cross-Region Replication
- Azure Backup, Azure Site Recovery
- Google Cloud Backup and Disaster Recovery
- Características y limitaciones de cada servicio
- Integración con otros servicios cloud

Configuración de replicación y redundancia

- Replicación síncrona y asíncrona
- Replicación entre regiones (cross-region replication)
- Configuración de redundancia de datos
- Validación de replicación
- Monitoreo de estado de replicación

Automatización de copias de seguridad

- Programación de backups automatizados
- Herramientas de orquestación de backups
- Integración con Infrastructure as Code
- Validación automática de integridad
- Alertas y notificaciones de fallos de backup

Pruebas y Simulacros de Recuperación ante Desastres

Tipos de simulacros de recuperación

- Simulacros de escritorio (tabletop exercises)
- Simulacros parciales (partial recovery tests)
- Simulacros completos (full recovery tests)
- Simulacros de failover
- Pruebas de procedimientos de comunicación

Ejecución y validación de simulacros

- Planificación de simulacros

- Documentación de resultados
- Validación de cumplimiento de RTO/RPO
- Identificación de debilidades en planes
- Registro de lecciones aprendidas

Mejora continua de planes de recuperación

- Análisis de resultados de simulacros
- Identificación de brechas en planes
- Actualización de procedimientos
- Incorporación de nuevas tecnologías
- Comunicación de mejoras a equipos

Validación e Integridad de Datos en Recuperación

Técnicas de validación de datos

- Checksums y hashes criptográficos
- Validación de integridad de backups
- Reconciliación de datos post-restauración
- Detección de corrupción de datos
- Herramientas de validación de integridad

Procedimientos de restauración segura

- Restauración en entornos aislados
- Validación de datos restaurados
- Procedimientos de cutover
- Rollback en caso de problemas
- Documentación de restauraciones

Cumplimiento normativo en recuperación

- Requisitos de auditoría en recuperación
- Trazabilidad de cambios durante recuperación
- Cumplimiento de regulaciones (GDPR, HIPAA, PCI-DSS)
- Documentación de cumplimiento
- Reportes de recuperación

Respuesta ante Incidentes y Recuperación Operativa

Procedimientos de respuesta ante incidentes

- Detección y escalada de incidentes
- Activación de planes de recuperación
- Comunicación durante incidentes
- Coordinación de equipos de respuesta
- Documentación de incidentes

Gestión de crisis y comunicación

- Comunicación clara durante recuperación
- Actualización de estado a stakeholders
- Gestión de expectativas
- Escalada de problemas
- Post-mortem y lecciones aprendidas

Capacidad de respuesta y resiliencia

- Toma de decisiones bajo presión
- Ejecución sistemática de procedimientos
- Validación de servicios restaurados
- Mejora continua de procesos
- Desarrollo de cultura de resiliencia

Habilidades actitudinales

- Rigor en planificación de recuperación
- Responsabilidad en protección de datos
- Capacidad de respuesta ante crisis
- Orientación a mejora continua de resiliencia

Justificación

Este bloque agrupa competencias de continuidad de negocio, copias de seguridad y recuperación ante desastres. Las competencias C14, C34 y C35 comparten el propósito común de garantizar resiliencia operativa y recuperación ante fallos. La coherencia funcional se basa en que todas requieren conocimiento de estrategias de backup, replicación de datos y planes de recuperación. Los entregables compatibles incluyen planes BCP/DRP, políticas de backup y procedimientos de recuperación. Las situaciones de evaluación incluyen diseño de planes de continuidad, implementación de backups automatizados y ejecución de simulacros de recuperación.

Ubicación en la progresión

Este bloque representa la preparación para escenarios de fallo y recuperación ante desastres. Los profesionales diseñan planes de continuidad de negocio (BCP) y recuperación ante desastres (DRP) definiendo claramente RTO y RPO. Implementan estrategias de backup automatizado con validación periódica de restauración. Diseñan políticas de retención de backups alineadas con requisitos regulatorios. Ejecutan simulacros de recuperación ante desastres con registro de resultados. Restauran servicios ante incidentes validando integridad de datos. Este bloque es crítico para operación confiable y cumplimiento de requisitos de disponibilidad.

Bloque 10 - Migración de Aplicaciones y Adopción Cloud

Objetivo pedagógico

Capacitar al profesional para planificar y ejecutar migraciones de aplicaciones a cloud, coordinando proyectos y liderando transformación organizativa.

Actividades

Actividad 10.1 Planificar y ejecutar migraciones de aplicaciones
Actividad 10.2 Definir estrategias de adopción cloud
Actividad 10.3 Gestionar cambios organizativos y capacitación en adopción cloud

Competencias

Competencias	Indicadores
C5 - Monitorear rendimiento de servicios cloud mediante métricas, trazas distribuidas y análisis de tendencias para garantizar cumplimiento de SLOs	Configuración de dashboards con indicadores clave (latencia, throughput, tasa de error) alineados con SLIs/SLOs Análisis de trazas distribuidas para identificar cuellos de botella en arquitecturas de microservicios Alertas automáticas configuradas con umbrales basados en histórico de rendimiento y patrones de anomalía
C12 - Planificar y ejecutar migraciones de aplicaciones a cloud seleccionando estrategias (rehost, replatform, refactor) según requisitos técnicos y empresariales	Análisis de aplicaciones existentes identificando dependencias, requisitos de rendimiento y restricciones de compatibilidad Plan de migración detallado con fases, cronograma, recursos y estrategia de rollback en caso de fallos Validación post-migración verificando funcionalidad, rendimiento, seguridad y cumplimiento de SLAs

Saberes asociados

Estrategias y Modelos de Migración Cloud

Modelos de migración

- Rehost (lift-and-shift)
- Replatform (lift-tinker-and-shift)
- Refactor (re-architect)
- Repurchase (cambio de aplicación)
- Retire (desmantelamiento)

Evaluación de aplicaciones para migración

- Análisis de dependencias de aplicaciones
- Identificación de requisitos técnicos
- Evaluación de compatibilidad cloud
- Mapeo de componentes heredados
- Análisis de riesgos de migración

Planificación de migraciones

- Definición de fases de migración

- Cronograma y hitos de proyecto
- Asignación de recursos
- Identificación de dependencias entre aplicaciones
- Planes de contingencia y rollback

Validación y Monitoreo Post-Migración

Validación funcional de aplicaciones migradas

- Pruebas de funcionalidad completa
- Validación de integraciones
- Verificación de datos
- Pruebas de rendimiento comparativas
- Validación de seguridad post-migración

Monitoreo de rendimiento post-migración

- Comparación de métricas pre y post-migración
- Identificación de degradación de rendimiento
- Análisis de latencia y throughput
- Monitoreo de disponibilidad
- Detección de anomalías

Validación de cumplimiento de SLAs

- Medición de SLIs post-migración
- Verificación de cumplimiento de SLOs
- Análisis de desviaciones
- Documentación de resultados
- Escalado de problemas de rendimiento

Coordinación de Proyectos de Migración

Gestión de cronograma y recursos

- Planificación de hitos de proyecto
- Asignación de recursos técnicos
- Gestión de capacidad de equipos
- Seguimiento de desviaciones
- Replanificación ante cambios

Gestión de riesgos en migraciones

- Identificación de riesgos técnicos
- Evaluación de impacto de riesgos
- Definición de estrategias de mitigación
- Monitoreo de riesgos
- Escalado de problemas críticos

Comunicación con stakeholders

- Reportes de estado de proyecto
- Comunicación de desviaciones
- Gestión de expectativas
- Escalado de problemas
- Documentación de decisiones

Liderazgo y Transformación Organizativa Cloud

Promoción de adopción de cloud

- Comunicación de beneficios de cloud
- Ejemplificación de nuevas prácticas
- Influencia positiva en equipos

- Resolución de resistencia al cambio
- Celebración de hitos de adopción

Capacitación y transferencia de conocimiento

- Identificación de necesidades de formación
- Diseño de programas de capacitación
- Facilitación de aprendizaje de equipos
- Documentación de procedimientos
- Mentoría de profesionales

Gestión del cambio organizativo

- Análisis de impacto organizativo
- Comunicación de cambios
- Apoyo a equipos en transición
- Medición de adopción
- Mejora continua de procesos

Herramientas y Plataformas de Migración Cloud

Herramientas de migración de aplicaciones

- AWS Application Migration Service (MGN)
- Azure Migrate
- Google Cloud Migrate for Compute Engine
- Herramientas de replicación de máquinas virtuales
- Herramientas de análisis de dependencias

Herramientas de migración de datos

- AWS DataSync
- Azure Data Box
- Google Cloud Transfer Service
- Herramientas de sincronización de datos
- Herramientas de validación de integridad

Plataformas de gestión de migraciones

- AWS Migration Accelerator Program (MAP)
- Azure Migration Program
- Herramientas de seguimiento de proyectos
- Dashboards de progreso de migración
- Herramientas de documentación

Métricas y Criterios de Éxito en Migraciones

KPIs de migración

- Porcentaje de aplicaciones migradas
- Tiempo promedio de migración por aplicación
- Tasa de éxito de migraciones
- Reducción de costes post-migración
- Mejora de rendimiento

Criterios de éxito técnico

- Cumplimiento de SLAs post-migración
- Validación de funcionalidad
- Seguridad equivalente o mejorada
- Integridad de datos verificada
- Disponibilidad alcanzada

Criterios de éxito empresarial

- Alineación con objetivos de negocio

- Retorno de inversión (ROI)
- Reducción de costes operativos
- Mejora de agilidad empresarial
- Satisfacción de usuarios finales

Habilidades actitudinales

- Planificación meticulosa de migraciones
- Comunicación clara durante transformación
- Liderazgo en adopción de cambios
- Responsabilidad en validación post-migración

Justificación

Este bloque agrupa competencias de migración de aplicaciones, coordinación de proyectos y liderazgo de transformación. Las competencias C5, C12, C18 y C19 comparten el propósito común de facilitar adopción de cloud en organizaciones. La coherencia funcional se basa en que todas requieren conocimiento de estrategias de migración, gestión de proyectos y cambio organizativo. Los entregables compatibles incluyen planes de migración, cronogramas de proyecto y programas de formación. Las situaciones de evaluación incluyen análisis de aplicaciones, ejecución de migraciones y coordinación de equipos.

Ubicación en la progresión

Este bloque representa la transformación organizativa hacia cloud. Los profesionales analizan aplicaciones existentes identificando dependencias y requisitos de compatibilidad. Seleccionan estrategias de migración (rehost, replatform, refactor) según requisitos técnicos y empresariales. Planifican migraciones detalladamente con fases, cronograma y recursos. Coordinan proyectos gestionando cronograma, recursos y riesgos. Lideran transformación organizativa promoviendo cambio cultural y capacitación. Monitorean rendimiento de aplicaciones migradas. Este bloque integra conocimientos técnicos con gestión de cambio para facilitar adopción exitosa de cloud.

Bloque 11 - Optimización de Costes y Recursos Cloud

Objetivo pedagógico

Capacitar al profesional para optimizar infraestructura cloud mediante rightsizing, gestión de instancias y análisis de costes.

Actividades

Actividad 11.1 Analizar uso de recursos y optimizar infraestructura cloud
Actividad 11.2 Gestionar costes y presupuestos cloud

Competencias

Competencias	Indicadores
C2 - Evaluar y seleccionar proveedores cloud públicos considerando capacidades técnicas, cumplimiento normativo y análisis económico para alinearse con estrategia empresarial	Matriz comparativa de proveedores (AWS, Azure, GCP) con criterios técnicos, de seguridad y costes Análisis de cumplimiento normativo (ISO 27001, SOC 2, GDPR) según requisitos del sector Recomendación fundamentada con análisis de coste total de propiedad (TCO) y retorno de inversión (ROI)
C16 - Optimizar infraestructura cloud mediante rightsizing, gestión de instancias reservadas y análisis de costes para maximizar eficiencia económica	Análisis de utilización de recursos identificando instancias sobredimensionadas o subutilizadas mediante herramientas de recomendación Implementación de estrategias de compra (instancias reservadas, spot instances, savings plans) alineadas con patrones de carga Reporte mensual de costes por servicio, proyecto o departamento con análisis de tendencias y oportunidades de ahorro

Saberes asociados

Análisis de Costes en Cloud

Modelos de precios cloud

- Precios bajo demanda
- Instancias reservadas
- Spot instances
- Savings plans
- Modelos de precios por servicio (AWS, Azure, GCP)

Herramientas de análisis de costes

- AWS Cost Explorer
- Azure Cost Management
- Google Cloud Billing
- Herramientas de terceros (CloudHealth, Cloudability)
- Análisis de costes por proyecto y departamento

Métricas de eficiencia económica

- Costo por unidad de computación
- Costo por transacción

- Costo total de propiedad (TCO)
- Retorno de inversión (ROI)
- Análisis de tendencias de costes

Optimización de Recursos Cloud

Rightsizing de instancias

- Análisis de utilización de CPU y memoria
- Identificación de instancias sobredimensionadas
- Identificación de instancias subutilizadas
- Recomendaciones de cambio de tipo de instancia
- Validación de impacto en rendimiento

Gestión de instancias reservadas

- Análisis de patrones de carga
- Selección de duración de reserva
- Gestión de cartera de instancias reservadas
- Conversión de instancias reservadas
- Análisis de ahorro vs. flexibilidad

Optimización de almacenamiento

- Políticas de ciclo de vida de datos
- Selección de tipos de almacenamiento económicos
- Compresión y deduplicación de datos
- Eliminación de datos redundantes
- Análisis de costes de almacenamiento

Automatización de optimización

- Herramientas de optimización automatizada
- Políticas de escalado automático
- Apagado automático de recursos no utilizados
- Alertas de anomalías de costes
- Reportes automatizados de optimización

Gobernanza de Costes Cloud

Políticas de control de costes

- Límites de presupuesto por proyecto
- Políticas de aprobación de recursos
- Etiquetado de recursos para seguimiento
- Asignación de costes a centros de coste
- Políticas de retención de datos

Reportes y comunicación de costes

- Reportes de costes por servicio
- Reportes de costes por proyecto
- Reportes de costes por departamento
- Análisis de desviaciones presupuestarias
- Comunicación de oportunidades de ahorro

Evaluación de proveedores cloud

- Comparación de precios entre proveedores
- Análisis de modelos de precios
- Evaluación de descuentos por volumen
- Análisis de costes de migración
- Evaluación de costes de salida (lock-in)

Métricas de Rendimiento y Utilización

Métricas de utilización de recursos

- Utilización de CPU
- Utilización de memoria
- Utilización de red
- Utilización de almacenamiento
- Métricas de I/O de disco

Análisis de tendencias

- Identificación de patrones de carga
- Proyección de crecimiento de costes
- Análisis de estacionalidad
- Detección de anomalías
- Análisis de correlación entre métricas

Economía de Cloud Computing

Modelos económicos de cloud

- Capex vs. Opex
- Economía de escala en cloud
- Ventajas económicas de cloud
- Costes ocultos de cloud
- Análisis de viabilidad económica

Estrategias de compra cloud

- Análisis de opciones de compra
- Negociación de descuentos
- Gestión de compromisos de gasto
- Optimización de mix de instancias
- Planificación de capacidad

Cultura de Optimización de Costes

Responsabilidad económica

- Conciencia de costes en decisiones técnicas
- Justificación económica de cambios
- Comunicación de impacto económico
- Rendición de cuentas de costes
- Alineación con presupuestos

Mejora continua de eficiencia

- Identificación de oportunidades de ahorro
- Implementación de mejoras de eficiencia
- Validación de resultados de optimización
- Documentación de lecciones aprendidas
- Compartir mejores prácticas de optimización

Habilidades actitudinales

- Orientación a eficiencia económica
- Rigor en análisis de datos de costes
- Comunicación clara de oportunidades de ahorro
- Responsabilidad en validación de cambios

Justificación

Este bloque agrupa competencias de optimización de costes, análisis de utilización y gestión de recursos. Las competencias C2, C16 y C25 comparten el propósito común de maximizar eficiencia económica de infraestructura cloud. La coherencia funcional se basa en que todas requieren análisis de utilización de recursos, evaluación de opciones de compra y reporte de costes. Los entregables compatibles incluyen análisis de rightsizing, recomendaciones de optimización y reportes de costes. Las situaciones de evaluación incluyen identificación de instancias sobredimensionadas, implementación de estrategias de compra y análisis de tendencias de costes.

Ubicación en la progresión

Este bloque representa la optimización continua de inversión en cloud. Los profesionales analizan utilización de recursos identificando instancias sobredimensionadas o subutilizadas. Implementan estrategias de compra (instancias reservadas, spot instances, savings plans) alineadas con patrones de carga. Realizan rightsizing de instancias validando impacto en rendimiento. Analizan costes detalladamente por servicio, proyecto o departamento. Identifican oportunidades de ahorro y proponen mejoras de eficiencia. Reportan costes y ahorros logrados a stakeholders. Este bloque habilita toma de decisiones informada sobre inversión en cloud.

Bloque 12 - Gestión de Proyectos, Documentación y Comunicación Cloud

Objetivo pedagógico

Capacitar al profesional para documentar arquitecturas cloud, coordinar proyectos y comunicar decisiones técnicas a stakeholders.

Actividades

Actividad 12.1 Coordinar y seguimiento de proyectos cloud
Actividad 12.2 Documentar configuraciones y decisiones de arquitectura cloud
Actividad 12.3 Comunicar estado operativo y facilitar colaboración en iniciativas cloud

Competencias

Competencias	Indicadores
C17 - Documentar arquitecturas cloud mediante decisiones arquitectónicas (ADRs) y runbooks operativos para facilitar mantenimiento y transferencia de conocimiento	Registro de decisiones arquitectónicas (ADRs) con contexto, alternativas evaluadas, decisión y consecuencias Documentación técnica de arquitectura con diagramas actualizados (C4, UML) y descripción de componentes y flujos Runbooks operativos con procedimientos paso a paso para tareas comunes (despliegue, escalado, recuperación ante incidentes)
C18 - Coordinar proyectos de adopción cloud gestionando cronograma, recursos y riesgos para asegurar entrega exitosa y alineación con objetivos empresariales	Plan de proyecto detallado con hitos, dependencias, asignación de recursos y presupuesto con seguimiento semanal Identificación y gestión de riesgos con planes de mitigación y escalación de problemas a stakeholders Comunicación periódica de estado a equipos técnicos y de negocio con métricas de progreso y desviaciones
C19 - Liderar transformación organizativa hacia cloud promoviendo cambio cultural, capacitación y adopción de nuevas prácticas entre equipos	Diseño e implementación de programas de formación cloud adaptados a roles (desarrolladores, operaciones, arquitectos) Establecimiento de comunidades de práctica y mentoring para compartir conocimiento y buenas prácticas Medición de adopción mediante encuestas, métricas de uso de servicios cloud y feedback de equipos
C20 - Alinear soluciones cloud con objetivos empresariales traduciendo requisitos de negocio a especificaciones técnicas para garantizar valor agregado	Análisis de requisitos empresariales documentando objetivos, restricciones y criterios de éxito cuantificables Traducción de objetivos de negocio a requisitos técnicos (disponibilidad, rendimiento, seguridad, costes) con métricas Evaluación de valor agregado mediante análisis de beneficios (reducción de costes, mejora de rendimiento, agilidad) post-implementación

Saberes asociados

Documentación Técnica de Arquitectura Cloud

Decisiones Arquitectónicas (ADRs)

- Estructura y componentes de un ADR
- Documentación de contexto y alternativas evaluadas
- Registro de consecuencias y trade-offs
- Versionado y evolución de decisiones

Documentación de Arquitectura Cloud

- Diagramas de arquitectura (C4, UML)
- Especificaciones técnicas de componentes
- Flujos de datos y integraciones
- Documentación de patrones arquitectónicos

Runbooks Operativos

- Procedimientos paso a paso para tareas operativas
- Guías de despliegue y escalado
- Procedimientos de recuperación ante incidentes
- Documentación de troubleshooting

Gestión de Proyectos Cloud

Planificación de Proyectos Cloud

- Definición de alcance y objetivos
- Estimación de cronograma y recursos
- Identificación de riesgos y planes de contingencia
- Desglose de tareas (WBS)

Seguimiento y Control de Proyectos

- Monitoreo de cronograma y presupuesto
- Gestión de desviaciones de proyecto
- Seguimiento de hitos y entregables
- Reportes de estado a stakeholders

Gestión de Riesgos en Proyectos Cloud

- Identificación de riesgos técnicos y organizativos
- Evaluación de probabilidad e impacto
- Planes de mitigación y contingencia
- Monitoreo continuo de riesgos

Comunicación Técnica y Gestión de Stakeholders

Comunicación de Decisiones Técnicas

- Explicación de decisiones arquitectónicas a audiencias técnicas
- Traducción de conceptos técnicos para audiencias no técnicas
- Uso de diagramas y visualizaciones
- Presentación de trade-offs y justificación de decisiones

Reportes de Estado y Métricas

- Reportes de progreso de proyecto
- Comunicación de desviaciones y problemas
- Presentación de métricas de rendimiento
- Escalado de problemas críticos

Gestión de Expectativas de Stakeholders

- Identificación de stakeholders y sus intereses
- Comunicación proactiva de cambios
- Gestión de conflictos y desacuerdos
- Alineación de expectativas con realidad técnica

Liderazgo y Transformación Organizativa Cloud

Liderazgo en Adopción de Cloud

- Promoción de cambio cultural hacia cloud
- Influencia positiva en adopción de nuevas prácticas
- Ejemplificación de comportamientos deseados
- Motivación de equipos en transformación

Gestión del Cambio Organizativo

- Identificación de resistencia al cambio
- Estrategias de comunicación para cambio
- Gestión de transiciones organizativas
- Medición de adopción y éxito de cambio

Transferencia de Conocimiento

- Diseño de programas de capacitación
- Documentación clara para aprendizaje
- Mentoría y coaching de equipos
- Aseguramiento de continuidad de conocimiento

Alineación de Soluciones Cloud con Objetivos Empresariales

Traducción de Requisitos de Negocio

- Comprensión de objetivos empresariales
- Identificación de requisitos funcionales y no funcionales
- Traducción de requisitos a especificaciones técnicas
- Validación de alineación con estrategia empresarial

Análisis de Valor Empresarial

- Cuantificación de beneficios empresariales
- Análisis de retorno de inversión (ROI)
- Identificación de KPIs de éxito
- Comunicación de valor agregado

Criterios de Éxito de Proyectos Cloud

- Definición de criterios técnicos de éxito
- Definición de criterios empresariales de éxito
- Métricas de cumplimiento de objetivos
- Validación post-proyecto de éxito

Herramientas y Prácticas de Colaboración en Proyectos Cloud

Herramientas de Gestión de Proyectos

- Plataformas de seguimiento de proyectos (Jira, Azure DevOps)
- Herramientas de documentación colaborativa
- Sistemas de control de versiones para documentación
- Herramientas de comunicación de equipo

Prácticas de Colaboración Efectiva

- Reuniones de coordinación y sincronización
- Documentación compartida y versionada
- Procesos de revisión y aprobación
- Gestión de dependencias entre equipos

Métricas y Dashboards de Proyecto

- Indicadores de progreso de proyecto
- Dashboards de estado para stakeholders
- Métricas de calidad de entregables
- Análisis de desviaciones

Habilidades actitudinales

- Rigor en documentación técnica
- Claridad en comunicación técnica
- Responsabilidad en coordinación de proyectos
- Orientación a transferencia de conocimiento

Justificación

Este bloque agrupa competencias de documentación, gestión de proyectos y comunicación. Las competencias C17, C18, C19 y C20 comparten el propósito común de facilitar comunicación y coordinación en iniciativas cloud. La coherencia funcional se basa en que todas requieren habilidades de documentación, gestión de proyectos y comunicación efectiva. Los entregables compatibles incluyen documentación técnica, planes de proyecto y reportes de estado. Las situaciones de evaluación incluyen creación de ADRs, coordinación de equipos y comunicación a stakeholders.

Ubicación en la progresión

Este bloque representa la dimensión de comunicación y coordinación en operación de servicios cloud. Los profesionales documentan arquitecturas mediante decisiones arquitectónicas (ADRs) y diagramas técnicos. Crean runbooks operativos con procedimientos paso a paso. Coordinan proyectos de adopción cloud gestionando cronograma, recursos y riesgos. Comunican estado regularmente a equipos técnicos y de negocio. Lideran transformación organizativa promoviendo cambio cultural. Alinean soluciones cloud con objetivos empresariales traduciendo requisitos de negocio a especificaciones técnicas. Este bloque es transversal a todos los aspectos de operación cloud y habilita transferencia de conocimiento.

ANEXO IV Marco de evaluación

ANEXO IV a. Exenciones de unidades

Profesional con certificación AWS Solutions Architect Associate o equivalente, exentos de realizar la unidad U1.

Profesional con certificación Azure Administrator o equivalente, exentos de realizar la unidad U2.

Profesional con certificación Kubernetes (CKA) o equivalente, exentos de realizar la unidad U3.

Profesional con experiencia demostrada de 3+ años en monitoreo y optimización de servicios cloud, exentos de realizar la unidad U4.

Profesional con certificación en administración de sistemas cloud (AWS SysOps, Azure Administrator), exentos de realizar la unidad U5.

Profesional con experiencia demostrada de 2+ años en integración de sistemas cloud, exentos de realizar la unidad U6.

Profesional con certificación en seguridad cloud (AWS Security, Azure Security Engineer), exentos de realizar la unidad U7.

Profesional con experiencia demostrada de 2+ años en gestión de datos y almacenamiento cloud, exentos de realizar la unidad U8.

Profesional con experiencia demostrada de 2+ años en continuidad de negocio y recuperación ante desastres, exentos de realizar la unidad U9.

Profesional con experiencia demostrada de 3+ años en migración de aplicaciones a cloud, exentos de realizar la unidad U10.

Profesional con experiencia demostrada de 2+ años en optimización de costes cloud, exentos de realizar la unidad U11.

Profesional con experiencia demostrada de 3+ años en gestión de proyectos cloud, exentos de realizar la unidad U12.

ANEXO IV b. Reglamento de examen

Pruebas	Unidad	Coef.	Forma	Duración
E1 Diseño de Arquitecturas Cloud Escalables y Evaluación de Proveedores	**U1**	**2**	Prueba escrita única	3h
E2 Provisión de Infraestructura Cloud y Configuración de Seguridad	**U2**	**2**	Prueba práctica única	4h
E3 Automatización, Orquestación de Contenedores e Integración Asíncrona	**U3**	**2**	Prueba práctica única	4h
E4 Monitoreo, Optimización de Costes y Gestión Operativa	**U4**	**2**	Prueba escrita única	3h
E5 Gestión de Servidores, Software y Orquestación de Contenedores	**U5**	**2**	Prueba práctica única	4h
E6 Integración de Sistemas, Arquitecturas de Mensajería y Coordinación de Proyectos	**U6**	**2**	Prueba escrita única	3h
E7 Seguridad Cloud, Controles de Seguridad y Cumplimiento Normativo	**U7**	**2**	Prueba escrita única	3h
E8 Almacenamiento, Datos y Bases de Datos Cloud	**U8**	**2**	Prueba escrita única	3h
E9 Continuidad de Negocio, Recuperación ante Desastres y Copias de Seguridad	**U9**	**2**	Prueba escrita única	3h
E10 Migración de Aplicaciones, Adopción Cloud y Liderazgo de Transformación	**U10**	**2**	Prueba escrita única	3h
E11 Optimización de Costes y Recursos Cloud	**U11**	**2**	Prueba escrita única	3h
E12 Documentación de Arquitecturas, Gestión de Proyectos y Comunicación Cloud	**U12**	**2**	Prueba escrita única	3h

*Pruebas optativas: solo se tienen en cuenta los puntos por encima de la media.

ANEXO IV c. Definición de las pruebas

E1 : Diseño de Arquitecturas Cloud Escalables y Evaluación de Proveedores

Finalidades de la prueba

Evaluar capacidad del profesional para diseñar arquitecturas cloud escalables aplicando patrones arquitectónicos modernos, evaluar proveedores cloud públicos y alinear soluciones con objetivos empresariales.

Contenido de la prueba

Diseño de arquitecturas escalables y resilientes; patrones arquitectónicos (microservicios, serverless, contenedores); evaluación de proveedores cloud (AWS, Azure, GCP); análisis técnico y económico; cumplimiento normativo; alineación de soluciones con objetivos empresariales; documentación de decisiones arquitectónicas.

Competencias evaluadas

C1 - Diseñar arquitecturas cloud escalables y resilientes aplicando patrones arquitectónicos modernos para satisfacer requisitos de disponibilidad y rendimiento

C2 - Evaluar y seleccionar proveedores cloud públicos considerando capacidades técnicas, cumplimiento normativo y análisis económico para alinearse con estrategia empresarial

C10 - Diseñar arquitecturas cloud híbridas estableciendo conectividad segura entre entornos on-premises y cloud para mantener flexibilidad operativa

C20 - Alinear soluciones cloud con objetivos empresariales traduciendo requisitos de negocio a especificaciones técnicas para garantizar valor agregado

Criterios de evaluación

- Diseña arquitecturas cloud que cumplen requisitos de escalabilidad y resiliencia aplicando patrones arquitectónicos apropiados
- Evalúa proveedores cloud considerando capacidades técnicas, cumplimiento normativo y análisis económico
- Documenta decisiones arquitectónicas con claridad, incluyendo alternativas evaluadas y justificación de selección
- Alinea soluciones cloud con objetivos empresariales traduciendo requisitos de negocio a especificaciones técnicas
- Analiza trade-offs arquitectónicos considerando impacto en disponibilidad, rendimiento, seguridad y costes

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Examen escrito con casos prácticos de diseño arquitectónico y evaluación de proveedores

Aprendizaje : Evaluación continua — Evaluación continua mediante proyectos de diseño arquitectónico en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en diseño y evaluación de arquitecturas cloud

Reglas específicas

- Se requiere presentación de al menos un caso de diseño arquitectónico documentado
- Evaluación incluye análisis de decisiones técnicas y justificación de alternativas
- Se valida comprensión de patrones arquitectónicos y su aplicación en contextos reales

E2 : Provisión de Infraestructura Cloud y Configuración de Seguridad

Finalidades de la prueba

Evaluar capacidad del profesional para provisionar servicios cloud públicos mediante IaC, configurar controles de seguridad, administrar ciclo de vida de instancias y gestionar identidades y accesos.

Contenido de la prueba

Provisión de servicios cloud públicos (AWS, Azure, GCP); herramientas de Infrastructure as Code (Terraform, CloudFormation, Pulumi); configuración de seguridad en cloud; hardening de servidores; gestión de identidades y accesos (IAM); principio de mínimo privilegio; administración del ciclo de vida de instancias.

Competencias evaluadas

C3 - Provisionar servicios cloud públicos mediante herramientas de Infrastructure as Code garantizando reproducibilidad, versionado y trazabilidad de configuraciones

C4 - Configurar controles de seguridad en entornos cloud aplicando modelo de responsabilidad compartida para proteger datos y servicios contra amenazas

C6 - Administrar ciclo de vida de instancias cloud aplicando hardening y configuración segura para garantizar disponibilidad y seguridad operativa

C15 - Administrar identidades y accesos en cloud aplicando principio de mínimo privilegio para controlar autorización y auditar acceso a recursos

Criterios de evaluación

- Provisiona servicios cloud públicos mediante herramientas IaC garantizando reproducibilidad y versionado
- Configura controles de seguridad aplicando modelo de responsabilidad compartida
- Administra ciclo de vida de instancias cloud aplicando hardening y configuración segura
- Implementa gestión de identidades y accesos aplicando principio de mínimo privilegio
- Valida configuraciones de seguridad contra estándares (CIS Benchmarks, ISO 27001)

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Prueba práctica de provisión de infraestructura y configuración de seguridad en entorno cloud

Aprendizaje : Evaluación continua — Evaluación continua mediante provisión de infraestructura en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en provisión y configuración de seguridad

Reglas específicas

- Se requiere demostración práctica de provisión mediante IaC
- Evaluación incluye validación de configuraciones de seguridad
- Se verifica cumplimiento de estándares de hardening

E3 : Automatización, Orquestación de Contenedores e Integración Asíncrona

Finalidades de la prueba

Evaluar capacidad del profesional para automatizar infraestructura cloud, orquestar contenedores con Kubernetes e implementar soluciones de mensajería asíncrona.

Contenido de la prueba

Automatización de infraestructura cloud; herramientas de IaC avanzadas (Terraform, Pulumi); orquestación de contenedores (Kubernetes); despliegue automatizado; escalado dinámico; soluciones de mensajería (SQS, SNS, Service Bus, Pub/Sub, Kafka); análisis de vulnerabilidades en pipelines (SAST/DAST); integración de seguridad en DevOps.

Competencias evaluadas

C7 - Orquestar contenedores en plataformas cloud utilizando Kubernetes para automatizar despliegue, escalado y gestión del ciclo de vida de aplicaciones

C9 - Aplicar prácticas de desarrollo seguro integrando análisis de vulnerabilidades en pipelines DevOps para identificar y mitigar riesgos de seguridad tempranamente

C11 - Implementar soluciones de mensajería y eventos en cloud diseñando arquitecturas asíncronas para desacoplamiento de componentes y escalabilidad

Criterios de evaluación

- Automatiza infraestructura cloud mediante herramientas IaC con validación exhaustiva
- Orquesta contenedores con Kubernetes automatizando despliegue, escalado y gestión del ciclo de vida
- Implementa soluciones de mensajería asíncrona para desacoplamiento de componentes
- Integra análisis de vulnerabilidades en pipelines DevOps mediante SAST/DAST
- Valida cambios automatizados antes de despliegue en producción

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Prueba práctica de automatización, orquestación de contenedores e implementación de mensajería

Aprendizaje : Evaluación continua — Evaluación continua mediante automatización en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en automatización y orquestación

Reglas específicas

- Se requiere demostración práctica de automatización con herramientas IaC
- Evaluación incluye orquestación de contenedores con Kubernetes
- Se valida integración de seguridad en pipelines DevOps

E4 : Monitoreo, Optimización de Costes y Gestión Operativa

Finalidades de la prueba

Evaluar capacidad del profesional para monitorear rendimiento de servicios cloud, optimizar infraestructura y costes, y gestionar operaciones con cumplimiento de SLAs.

Contenido de la prueba

Monitoreo de rendimiento (APM, métricas, trazas distribuidas); definición de SLIs y SLOs; análisis de tendencias de rendimiento; optimización de infraestructura (rightsizing, instancias reservadas, spot instances); análisis de costes; gestión operativa; cumplimiento de SLAs; procedimientos operativos estándar (SOPs).

Competencias evaluadas

C5 - Monitorear rendimiento de servicios cloud mediante métricas, trazas distribuidas y análisis de tendencias para garantizar cumplimiento de SLOs

C16 - Optimizar infraestructura cloud mediante rightsizing, gestión de instancias reservadas y análisis de costes para maximizar eficiencia económica

Criterios de evaluación

- Monitorea rendimiento de servicios cloud mediante métricas, trazas distribuidas y análisis de tendencias
- Define SLIs y SLOs alineados con requisitos empresariales
- Optimiza infraestructura mediante rightsizing y gestión de instancias
- Analiza costes detalladamente e identifica oportunidades de ahorro
- Gestiona operaciones asegurando cumplimiento de SLAs

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Examen escrito con análisis de casos de monitoreo y optimización

Aprendizaje : Evaluación continua — Evaluación continua mediante análisis de monitoreo en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en monitoreo y optimización

Reglas específicas

- Se requiere presentación de dashboards de monitoreo configurados
- Evaluación incluye análisis de costes y recomendaciones de optimización
- Se valida cumplimiento de SLAs en casos prácticos

E5 : Gestión de Servidores, Software y Orquestación de Contenedores

Finalidades de la prueba

Evaluar capacidad del profesional para administrar ciclo de vida de instancias cloud, orquestar contenedores y gestionar software en entornos cloud.

Contenido de la prueba

Administración del ciclo de vida de instancias cloud; hardening y configuración segura de servidores; monitoreo de estado y rendimiento; orquestación de contenedores (Kubernetes); gestión del ciclo de vida de aplicaciones; herramientas de gestión de configuración (Ansible, Chef, Puppet); escalado automático.

Competencias evaluadas

C6 - Administrar ciclo de vida de instancias cloud aplicando hardening y configuración segura para garantizar disponibilidad y seguridad operativa

C7 - Orquestar contenedores en plataformas cloud utilizando Kubernetes para automatizar despliegue, escalado y gestión del ciclo de vida de aplicaciones

Criterios de evaluación

- Administra ciclo de vida completo de instancias cloud desde provisión hasta desaprovisionamiento
- Aplica hardening y configuración segura de servidores
- Monitorea estado y rendimiento de servidores
- Orquesta contenedores con Kubernetes automatizando despliegue y escalado
- Gestiona software mediante herramientas de configuración

Forma de evaluación

Vía escolar pública o privada concertada : Prueba práctica única — Prueba práctica de administración de instancias y orquestación de contenedores

Aprendizaje : Evaluación continua — Evaluación continua mediante gestión de servidores en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en gestión de servidores y contenedores

Reglas específicas

- Se requiere demostración práctica de administración de instancias
- Evaluación incluye orquestación de contenedores
- Se valida aplicación de hardening de servidores

E6 : Integración de Sistemas, Arquitecturas de Mensajería y Coordinación de Proyectos

Finalidades de la prueba

Evaluar capacidad del profesional para integrar soluciones cloud con sistemas heredados, diseñar arquitecturas de mensajería y coordinar proyectos de integración.

Contenido de la prueba

Integración de sistemas cloud con legados; APIs y patrones de integración; colas de mensajes y buses de eventos; arquitecturas asíncronas; documentación de flujos de integración; coordinación de proyectos; gestión de cronograma y recursos; comunicación con stakeholders.

Competencias evaluadas

C8 - Integrar soluciones cloud con sistemas heredados mediante APIs, colas de mensajes y buses de eventos para garantizar interoperabilidad y consistencia de datos

C11 - Implementar soluciones de mensajería y eventos en cloud diseñando arquitecturas asíncronas para desacoplamiento de componentes y escalabilidad

C18 - Coordinar proyectos de adopción cloud gestionando cronograma, recursos y riesgos para asegurar entrega exitosa y alineación con objetivos empresariales

Criterios de evaluación

- Integra soluciones cloud con sistemas heredados mediante APIs y patrones de integración
- Diseña arquitecturas de mensajería asíncrona para desacoplamiento de componentes
- Documenta flujos de integración con claridad
- Coordina proyectos de integración gestionando cronograma y recursos
- Valida integridad de datos en flujos de integración

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Examen escrito con diseño de integraciones y coordinación de proyectos

Aprendizaje : Evaluación continua — Evaluación continua mediante proyectos de integración en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en integración de sistemas

Reglas específicas

- Se requiere presentación de diseño de integración documentado
- Evaluación incluye análisis de patrones de integración
- Se valida coordinación de proyectos de integración

E7 : Seguridad Cloud, Controles de Seguridad y Cumplimiento Normativo

Finalidades de la prueba

Evaluar capacidad del profesional para garantizar seguridad de servicios cloud, aplicar controles de seguridad, gestionar identidades y accesos, y promover cultura de seguridad.

Contenido de la prueba

Configuración de controles de seguridad en cloud; modelo de responsabilidad compartida; análisis de vulnerabilidades (SAST/DAST); gestión de identidades y accesos (IAM); principio de mínimo privilegio; cumplimiento normativo (ISO 27001, SOC 2, CIS Benchmarks); evaluación de postura de seguridad; promoción de cultura de seguridad; formación en seguridad.

Competencias evaluadas

C4 - Configurar controles de seguridad en entornos cloud aplicando modelo de responsabilidad compartida para proteger datos y servicios contra amenazas

C9 - Aplicar prácticas de desarrollo seguro integrando análisis de vulnerabilidades en pipelines DevOps para identificar y mitigar riesgos de seguridad tempranamente

C15 - Administrar identidades y accesos en cloud aplicando principio de mínimo privilegio para controlar autorización y auditar acceso a recursos

Criterios de evaluación

- Configura controles de seguridad aplicando modelo de responsabilidad compartida
- Implementa gestión de identidades y accesos con principio de mínimo privilegio
- Integra análisis de vulnerabilidades en pipelines DevOps
- Evalúa postura de seguridad contra estándares
- Promueve cultura de seguridad mediante formación y guías

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Examen escrito con análisis de seguridad y cumplimiento normativo

Aprendizaje : Evaluación continua — Evaluación continua mediante evaluación de seguridad en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en seguridad cloud

Reglas específicas

- Se requiere presentación de evaluación de postura de seguridad
- Evaluación incluye análisis de cumplimiento normativo
- Se valida implementación de controles de seguridad

E8 : Almacenamiento, Datos y Bases de Datos Cloud

Finalidades de la prueba

Evaluar capacidad del profesional para diseñar soluciones de almacenamiento cloud, migrar datos y gestionar bases de datos gestionadas.

Contenido de la prueba

Diseño de soluciones de almacenamiento cloud; tipos de almacenamiento (objeto, bloque, archivo); migración de datos; validación de integridad de datos; políticas de ciclo de vida; bases de datos gestionadas; optimización de costes de almacenamiento; seguridad de datos.

Competencias evaluadas

C1 - Diseñar arquitecturas cloud escalables y resilientes aplicando patrones arquitectónicos modernos para satisfacer requisitos de disponibilidad y rendimiento

C13 - Migrar datos a cloud garantizando integridad, seguridad y validación mediante procesos automatizados y reconciliación de datos

Criterios de evaluación

- Diseña soluciones de almacenamiento cloud seleccionando tipos apropiados
- Migra datos a cloud garantizando integridad mediante validaciones
- Implementa políticas de ciclo de vida de datos
- Configura bases de datos gestionadas
- Optimiza costes de almacenamiento

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Examen escrito con diseño de soluciones de almacenamiento

Aprendizaje : Evaluación continua — Evaluación continua mediante proyectos de almacenamiento en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en almacenamiento y datos

Reglas específicas

- Se requiere presentación de diseño de solución de almacenamiento
- Evaluación incluye plan de migración de datos

- Se valida validación de integridad de datos

E9 : Continuidad de Negocio, Recuperación ante Desastres y Copias de Seguridad

Finalidades de la prueba

Evaluar capacidad del profesional para diseñar planes de continuidad de negocio, implementar copias de seguridad y restaurar servicios ante incidentes.

Contenido de la prueba

Planes de continuidad de negocio (BCP); planes de recuperación ante desastres (DRP); definición de RTO y RPO; estrategias de backup; validación de restauración; procedimientos de recuperación; simulacros de recuperación; resiliencia operativa.

Competencias evaluadas

C14 - Diseñar e implementar planes de continuidad de negocio y recuperación ante desastres definiendo RTO y RPO para garantizar resiliencia operativa

Criterios de evaluación

- Diseña planes de continuidad de negocio exhaustivos
- Define RTO y RPO alineados con requisitos empresariales
- Implementa estrategias de backup automatizado
- Valida capacidad de restauración mediante simulacros
- Ejecuta procedimientos de recuperación ante incidentes

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Examen escrito con diseño de planes de continuidad y recuperación

Aprendizaje : Evaluación continua — Evaluación continua mediante planes de continuidad en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en continuidad y recuperación

Reglas específicas

- Se requiere presentación de plan de continuidad documentado
- Evaluación incluye definición de RTO y RPO
- Se valida ejecución de simulacros de recuperación

E10 : Migración de Aplicaciones, Adopción Cloud y Liderazgo de Transformación

Finalidades de la prueba

Evaluar capacidad del profesional para planificar y ejecutar migraciones de aplicaciones a cloud, coordinar proyectos y liderar transformación organizativa.

Contenido de la prueba

Análisis de aplicaciones para migración; estrategias de migración (rehost, replatform, refactor); planificación de migraciones; coordinación de proyectos; gestión de cronograma y recursos; validación post-migración; liderazgo de transformación; cambio cultural; capacitación de equipos; comunicación a stakeholders.

Competencias evaluadas

C12 - Planificar y ejecutar migraciones de aplicaciones a cloud seleccionando estrategias (rehost, replatform, refactor) según requisitos técnicos y empresariales

C18 - Coordinar proyectos de adopción cloud gestionando cronograma, recursos y riesgos para asegurar entrega exitosa y alineación con objetivos empresariales

C19 - Liderar transformación organizativa hacia cloud promoviendo cambio cultural, capacitación y adopción de nuevas prácticas entre equipos

Criterios de evaluación

- Analiza aplicaciones identificando dependencias y requisitos de compatibilidad
- Selecciona estrategias de migración apropiadas
- Planifica migraciones detalladamente con fases y cronograma
- Coordina proyectos gestionando cronograma y recursos
- Lidera transformación organizativa promoviendo cambio cultural

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Examen escrito con planificación de migración y coordinación de proyectos

Aprendizaje : Evaluación continua — Evaluación continua mediante proyectos de migración en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en migración y transformación

Reglas específicas

- Se requiere presentación de plan de migración documentado
- Evaluación incluye análisis de aplicaciones
- Se valida coordinación de proyectos de migración

E11 : Optimización de Costes y Recursos Cloud

Finalidades de la prueba

Evaluar capacidad del profesional para optimizar infraestructura cloud mediante rightsizing, gestión de instancias y análisis de costes.

Contenido de la prueba

Análisis de utilización de recursos; rightsizing de instancias; gestión de instancias reservadas; spot instances; análisis de costes; identificación de oportunidades de ahorro; reporte de costes; optimización de servicios; eficiencia económica.

Competencias evaluadas

C16 - Optimizar infraestructura cloud mediante rightsizing, gestión de instancias reservadas y análisis de costes para maximizar eficiencia económica

Criterios de evaluación

- Analiza utilización de recursos identificando instancias sobredimensionadas
- Implementa estrategias de rightsizing validando impacto en rendimiento
- Selecciona opciones de compra (reservadas, spot) alineadas con patrones de carga
- Analiza costes detalladamente por servicio y proyecto
- Propone mejoras de eficiencia económica con cuantificación de ahorros

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Examen escrito con análisis de costes y optimización

Aprendizaje : Evaluación continua — Evaluación continua mediante análisis de costes en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en optimización de costes

Reglas específicas

- Se requiere presentación de análisis de costes
- Evaluación incluye recomendaciones de optimización
- Se valida cuantificación de ahorros potenciales

E12 : Documentación de Arquitecturas, Gestión de Proyectos y Comunicación Cloud

Finalidades de la prueba

Evaluar capacidad del profesional para documentar arquitecturas cloud, coordinar proyectos y comunicar decisiones técnicas a stakeholders.

Contenido de la prueba

Documentación técnica de arquitectura; decisiones arquitectónicas (ADRs); runbooks operativos; coordinación de proyectos; gestión de cronograma y recursos; comunicación a stakeholders; liderazgo de transformación; transferencia de conocimiento; alineación con objetivos empresariales.

Competencias evaluadas

C17 - Documentar arquitecturas cloud mediante decisiones arquitectónicas (ADRs) y runbooks operativos para facilitar mantenimiento y transferencia de conocimiento

C18 - Coordinar proyectos de adopción cloud gestionando cronograma, recursos y riesgos para asegurar entrega exitosa y alineación con objetivos empresariales

C20 - Alinear soluciones cloud con objetivos empresariales traduciendo requisitos de negocio a especificaciones técnicas para garantizar valor agregado

Criterios de evaluación

- Documenta arquitecturas mediante decisiones arquitectónicas (ADRs) con claridad
- Crea runbooks operativos con procedimientos paso a paso
- Coordina proyectos gestionando cronograma y recursos

- Comunica decisiones técnicas de forma comprensible para audiencias técnicas y no técnicas
- Alinea soluciones cloud con objetivos empresariales

Forma de evaluación

Vía escolar pública o privada concertada : Prueba escrita única — Examen escrito con documentación de arquitectura y comunicación

Aprendizaje : Evaluación continua — Evaluación continua mediante documentación en contexto laboral

Vae : Prueba oral única — Entrevista técnica sobre experiencia en documentación y comunicación

Reglas específicas

- Se requiere presentación de documentación técnica
- Evaluación incluye ADRs y runbooks
- Se valida claridad de comunicación a stakeholders

ANEXO IV d. Dispositivo de evaluación detallado por bloque

Este anexo describe, para cada bloque de competencias, el dispositivo de evaluación detallado: indicadores SMART por misión profesional, situaciones de evaluación (simulaciones, estudios de caso), pruebas esperadas (producciones documentales, acciones observables, elementos reflexivos), criterios de éxito agrupados en siete familias, y el umbral de validación del bloque. Este dispositivo constituye la referencia para evaluadores y tribunales.

Bloque 1 - Diseño y Evaluación de Arquitecturas Cloud

Indicadores de desempeño por misión

Misión	Indicadores SMART
M01 — Diseñar arquitecturas cloud escalables	Número de patrones arquitectónicos aplicados correctamente en diseño Porcentaje de requisitos de escalabilidad y resiliencia cubiertos por arquitectura Completitud de documentación arquitectónica (diagramas, especificaciones, ADRs) Validación de arquitectura contra marcos de referencia (AWS Well-Architected, Azure Architecture)
M02 — Configurar entornos cloud públicos	Número de criterios de evaluación aplicados en análisis de proveedores Cobertura de aspectos técnicos, económicos y de cumplimiento en evaluación Precisión de análisis TCO comparativo entre proveedores Alineación de recomendación de proveedor con requisitos empresariales
M08 — Construir arquitecturas tecnológicas flexibles	Número de marcos de referencia aplicados en diseño de arquitectura Porcentaje de requisitos de flexibilidad y resiliencia cubiertos Frecuencia de revisiones y mejoras de arquitectura Documentación de decisiones de arquitectura y trade-offs
M14 — Definir estrategias de adopción de cloud	Número de estrategias de adopción cloud evaluadas Cobertura de modelos de migración en plan de adopción Definición clara de KPIs y criterios de éxito Alineación de estrategia con objetivos empresariales

Situaciones de evaluación

Diseño de Arquitectura Cloud Escalable para Aplicación de E-commerce

Contexto : Una empresa de comercio electrónico requiere migrar su plataforma monolítica a cloud. La aplicación debe soportar picos de tráfico durante campañas de ventas (10x aumento de carga), mantener disponibilidad 99.99%, procesar millones de transacciones diarias y cumplir con regulaciones de protección de datos (GDPR, PCI-DSS). La empresa tiene presupuesto limitado y requiere optimización de costes.

Restricciones : Tiempo de diseño máximo 2 semanas, debe considerar al menos 3 patrones arquitectónicos diferentes, debe incluir análisis de costes estimados, debe documentar decisiones con justificación clara

Producciones esperadas :

- Diagrama de arquitectura detallado con componentes y flujos de datos
- Especificación técnica de cada componente (servicios, bases de datos, colas de mensajes)
- Análisis de escalabilidad demostrando cómo se alcanza 99.99% de disponibilidad
- Matriz de evaluación de patrones arquitectónicos (microservicios vs serverless vs contenedores)
- Estimación de costes mensuales por componente
- ADRs documentando decisiones principales y trade-offs
- Plan de migración de datos desde monolito a nueva arquitectura

Competencias evaluadas : C1, C20

Evaluación Comparativa de Proveedores Cloud Públicos

Contexto : Una organización financiera debe seleccionar proveedor cloud para modernizar su infraestructura de datos. Requiere cumplimiento estricto de regulaciones (HIPAA, SOC 2 Type II), baja latencia en región específica, capacidades avanzadas de análisis de datos, y optimización de costes. Debe evaluar AWS, Azure y GCP considerando aspectos técnicos, económicos y de cumplimiento.

Restricciones : Análisis debe cubrir mínimo 15 criterios de evaluación, debe incluir análisis TCO detallado, debe validar certificaciones de cumplimiento, debe documentar trade-offs entre proveedores

Producciones esperadas :

- Matriz de evaluación de proveedores con criterios técnicos, económicos y de cumplimiento
- Análisis TCO comparativo para 3 años de operación
- Validación de certificaciones y cumplimiento normativo de cada proveedor
- Comparativa de capacidades de servicios (bases de datos, análisis, seguridad)
- Análisis de disponibilidad de regiones y latencia
- Recomendación fundamentada con justificación clara
- Documento de riesgos y mitigaciones por proveedor

Competencias evaluadas : C2, C20

Diseño de Arquitectura Cloud Híbrida con Conectividad Segura

Contexto : Una empresa manufacturera requiere arquitectura híbrida que integre sistemas on-premises (ERP, MES) con servicios cloud (análisis de datos, machine learning, aplicaciones web). Debe mantener baja latencia entre entornos, garantizar seguridad de datos sensibles, cumplir con regulaciones de privacidad, y permitir escalabilidad de cargas de trabajo en cloud.

Restricciones : Debe diseñar conectividad segura entre entornos, debe especificar gestión de identidades híbrida, debe documentar sincronización de datos, debe incluir plan de recuperación ante fallos de conectividad

Producciones esperadas :

- Diagrama de arquitectura híbrida mostrando on-premises y cloud
- Especificación de conectividad (VPN, conexión dedicada, peering)
- Diseño de gestión de identidades federada
- Estrategia de replicación y sincronización de datos
- Análisis de seguridad y cumplimiento normativo
- Plan de recuperación ante fallos de conectividad
- Estimación de costes de conectividad y servicios cloud

Competencias evaluadas : C1, C10, C20

Alineación de Requisitos Empresariales con Especificaciones Técnicas Cloud

Contexto : Un banco requiere modernizar su plataforma de banca digital. Requisitos empresariales incluyen: reducir tiempo de lanzamiento de nuevos productos de 6 meses a 2 semanas, mejorar experiencia de cliente con latencia <100ms, reducir costes operativos 30%, cumplir con regulaciones bancarias (Basilea III, GDPR). Debe traducir estos requisitos a especificaciones técnicas cloud.

Restricciones : Debe mapear cada requisito empresarial a capacidades técnicas, debe cuantificar impacto de decisiones técnicas en objetivos empresariales, debe documentar criterios de éxito medibles

Producciones esperadas :

- Matriz de mapeo requisitos empresariales a capacidades técnicas
- Especificación técnica detallada de solución cloud
- Análisis de impacto en tiempo de lanzamiento de productos
- Estimación de mejora en latencia y experiencia de usuario
- Análisis de reducción de costes operativos
- Plan de cumplimiento normativo
- KPIs y criterios de éxito medibles
- Justificación económica con ROI estimado

Competencias evaluadas : C1, C2, C20

Revisión y Mejora Continua de Arquitectura Cloud Existente

Contexto : Una empresa tecnológica tiene arquitectura cloud en producción desde 2 años. Requiere revisar arquitectura para identificar oportunidades de mejora en rendimiento, seguridad, costes y escalabilidad. Debe evaluar si arquitectura actual sigue siendo óptima o requiere refactorización.

Restricciones : Debe aplicar marcos de referencia (AWS Well-Architected, Azure Architecture), debe analizar métricas de rendimiento y costes actuales, debe identificar al menos 5 oportunidades de mejora, debe priorizar mejoras por impacto e inversión

Producciones esperadas :

- Análisis de arquitectura actual contra marcos de referencia
- Identificación de debilidades y oportunidades de mejora
- Propuestas de refactorización con análisis de impacto
- Estimación de costes y beneficios de mejoras
- Plan de implementación priorizado
- Análisis de riesgos de cambios propuestos
- Métricas de éxito para validar mejoras

Competencias evaluadas : C1, C8

Pruebas esperadas

■ Pruebas documentales

- Diagramas de arquitectura cloud (componentes, flujos de datos, despliegue)
- Especificaciones técnicas detalladas de componentes y servicios
- Registros de decisiones arquitectónicas (ADRs) con contexto, alternativas y justificación
- Matrices de evaluación de patrones arquitectónicos o proveedores
- Análisis de escalabilidad y rendimiento
- Análisis TCO (Total Cost of Ownership) comparativo
- Documentación de cumplimiento normativo y certificaciones
- Planes de migración o adopción cloud
- Reportes de revisión arquitectónica contra marcos de referencia

■ Pruebas de acción (en campo)

- Presentación de propuesta arquitectónica a stakeholders técnicos y empresariales
- Defensa de decisiones arquitectónicas ante cuestionamientos
- Facilitación de sesiones de diseño arquitectónico con equipos multidisciplinares
- Validación de arquitectura contra requisitos mediante checklist
- Prototipado de componentes críticos para validar viabilidad
- Participación en revisiones de arquitectura con pares
- Comunicación de trade-offs y restricciones a stakeholders

■ Pruebas reflexivas

- Análisis de decisiones arquitectónicas tomadas y su impacto
- Reflexión sobre alternativas rechazadas y por qué
- Evaluación de alineación de arquitectura con objetivos empresariales
- Análisis de riesgos identificados y mitigaciones implementadas
- Reflexión sobre lecciones aprendidas de arquitecturas anteriores
- Evaluación de completitud y claridad de documentación
- Análisis de feedback recibido y mejoras incorporadas

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Arquitectura cumple con regulaciones y estándares aplicables (GDPR, HIPAA, PCI-DSS, ISO 27001, SOC 2)	Checklist de cumplimiento completado, certificaciones validadas, auditoría de cumplimiento aprobada
Qualité	Arquitectura es escalable, resiliente y cumple con requisitos de disponibilidad y rendimiento especificados	Análisis de escalabilidad validado, SLOs definidos y alcanzables, patrones de resiliencia implementados
Comunicación	Decisiones arquitectónicas se comunican claramente a audiencias técnicas y no técnicas con justificación fundamentada	Documentación completa y comprensible, presentaciones efectivas, feedback positivo de stakeholders
Pertinence	Solución arquitectónica se alinea con objetivos empresariales y requisitos técnicos especificados	Mapeo de requisitos a solución completo, ROI estimado positivo, criterios de éxito alcanzables
Cohérence	Componentes arquitectónicos están integrados coherentemente sin redundancias innecesarias ni conflictos	Diagrama de arquitectura coherente, interfaces bien definidas, flujos de datos claros
Traçabilité	Todas las decisiones arquitectónicas están documentadas con contexto, alternativas evaluadas y justificación clara	ADRs completos, matriz de evaluación de alternativas, documentación de trade-offs
Posture	Profesional demuestra pensamiento sistémico, rigor en evaluación de alternativas y orientación a valor empresarial	Análisis exhaustivo de alternativas, consideración de impacto a largo plazo, vinculación de decisiones técnicas con beneficios empresariales

Umbral de validación : Promedio ≥ 10/20

Bloque 2 - Provisión y Configuración de Infraestructura Cloud

Indicadores de desempeño por misión

Misión	Indicadores SMART
M02 — Configurar entornos cloud públicos	Número de servicios cloud públicos provisionados correctamente mediante IaC en el primer intento Porcentaje de configuraciones de seguridad que cumplen con estándares CIS Benchmarks Tiempo medio de provisión de entornos cloud desde solicitud hasta disponibilidad Número de vulnerabilidades de seguridad identificadas en auditorías post-provisión
M04 — Gestionar servidores en la nube	Porcentaje de instancias cloud que cumplen con estándares de hardening Tiempo medio de respuesta ante cambios de configuración de seguridad Número de accesos revocados por incumplimiento de mínimo privilegio Disponibilidad de instancias cloud (uptime porcentual)
M11 — Automatizar tareas de infraestructura cloud	Porcentaje de infraestructura definida como código (IaC) Número de cambios de infraestructura automatizados exitosamente Tiempo de ejecución de scripts de automatización Tasa de errores en ejecución de automatización

Situaciones de evaluación

Provisión de Entorno Cloud Seguro con IaC

Contexto : Una empresa necesita provisionar un entorno cloud completo en AWS para una nueva aplicación web. El entorno debe incluir una VPC con subredes públicas y privadas, instancias EC2 con hardening aplicado, grupos de seguridad configurados, y gestión de accesos IAM con principio de mínimo privilegio. Todo debe ser definido mediante Terraform para garantizar reproducibilidad y versionado.

Restricciones : Debe cumplir con CIS Benchmarks para AWS, implementar cifrado en tránsito y en reposo, y documentar todas las decisiones de configuración de seguridad.

Producciones esperadas :

- Código Terraform modular y versionado en repositorio Git
- Documentación de arquitectura de red y seguridad
- Políticas IAM granulares con principio de mínimo privilegio
- Reporte de validación de cumplimiento de estándares de seguridad
- Runbook de operación del entorno

Competencias evaluadas : C3, C4, C6, C15

Implementación de Hardening de Servidores Cloud

Contexto : Se requiere configurar un conjunto de instancias EC2 en AWS aplicando estándares de hardening. Las instancias deben ejecutar aplicaciones críticas y cumplir con requisitos de seguridad ISO 27001. Se debe implementar monitoreo de integridad de configuración y auditoría de cambios.

Restricciones : Todas las configuraciones deben ser validadas contra CIS Benchmarks, documentadas exhaustivamente y auditables. Se debe mantener trazabilidad completa de cambios.

Producciones esperadas :

- Imágenes de máquina virtual (AMI) endurecidas y documentadas
- Configuración de firewall del sistema operativo
- Políticas de auditoría y logging
- Reporte de validación de hardening
- Procedimientos de mantenimiento y parches de seguridad

Competencias evaluadas : C6, C4

Configuración de Gestión de Identidades y Accesos (IAM)

Contexto : Una organización necesita implementar un sistema de gestión de identidades y accesos en Azure para controlar acceso a recursos cloud. Se requiere implementar autenticación multifactor, federación con directorio corporativo, y auditoría completa de accesos. Diferentes equipos (desarrollo, operaciones, seguridad) requieren diferentes niveles de acceso.

Restricciones : Debe aplicarse principio de mínimo privilegio, implementar MFA obligatoria, y mantener auditoría completa de accesos. Todas las políticas deben ser documentadas y revisables.

Producciones esperadas :

- Estructura de roles y políticas IAM granulares
- Configuración de federación de identidades
- Políticas de autenticación multifactor
- Reporte de auditoría de accesos
- Procedimientos de revisión periódica de accesos

Competencias evaluadas : C15, C4

Automatización de Provisión de Infraestructura Cloud

Contexto : Se necesita automatizar la provisión de múltiples entornos cloud (desarrollo, pruebas, producción) en GCP. Cada entorno debe ser idéntico en configuración pero con diferentes niveles de recursos. La automatización debe permitir despliegue rápido y reproducible de entornos completos.

Restricciones : Código IaC debe ser modular, reutilizable y versionado. Debe incluir validación de configuración antes de despliegue y permitir rollback de cambios. Todas las variables deben ser documentadas.

Producciones esperadas :

- Módulos Terraform reutilizables para cada componente
- Variables y configuraciones parametrizadas
- Scripts de validación y prueba de infraestructura
- Documentación de uso de módulos
- Procedimientos de despliegue y rollback

Competencias evaluadas : C3, C6

Auditoría de Postura de Seguridad Cloud

Contexto : Se requiere realizar una auditoría completa de postura de seguridad en un entorno AWS existente. Se deben identificar desviaciones de configuración, vulnerabilidades de seguridad, y accesos excesivos. Se debe generar reporte detallado con recomendaciones de remediación.

Restricciones : Auditoría debe cubrir configuración de instancias, políticas IAM, segmentación de red y cifrado. Todas las desviaciones deben ser documentadas con severidad y recomendaciones de remediación.

Producciones esperadas :

- Reporte de auditoría de postura de seguridad
- Matriz de desviaciones identificadas
- Recomendaciones de remediación priorizadas
- Plan de acción para corrección
- Procedimientos de validación post-remediación

Competencias evaluadas : C4, C6, C15

Pruebas esperadas

■ Pruebas documentales

- Código IaC versionado en repositorio Git con historial de cambios
- Documentación de arquitectura de red y seguridad
- Políticas IAM documentadas y justificadas
- Reportes de validación de cumplimiento de estándares
- Runbooks operativos con procedimientos paso a paso
- Decisiones arquitectónicas (ADRs) documentadas
- Auditorías de postura de seguridad
- Matrices de trazabilidad de configuraciones

■ Pruebas de acción (en campo)

- Provisión de servicios cloud mediante herramientas IaC
- Aplicación de hardening a instancias cloud
- Configuración de controles de seguridad (cifrado, segmentación de red)
- Implementación de políticas IAM con mínimo privilegio
- Validación de configuraciones contra estándares de seguridad
- Ejecución de auditorías de postura de seguridad
- Remediación de vulnerabilidades identificadas
- Monitoreo de cambios de configuración

■ Pruebas reflexivas

- Análisis de decisiones de configuración de seguridad tomadas
- Evaluación de trade-offs entre seguridad y facilidad de uso
- Reflexión sobre lecciones aprendidas en provisión de infraestructura
- Análisis de incidentes de seguridad y mejoras implementadas
- Evaluación de efectividad de controles de seguridad implementados
- Reflexión sobre evolución de estándares de seguridad
- Análisis de impacto de cambios de configuración en operaciones
- Evaluación de mejoras continuas en procesos de provisión

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Todas las configuraciones de infraestructura cumplen con estándares de seguridad aplicables (CIS Benchmarks, ISO 27001, SOC 2)	Porcentaje de configuraciones que pasan validación contra estándares (objetivo: 100%)
Qualité	Código IaC es modular, reutilizable, bien documentado y sigue mejores prácticas de programación	Revisión de código por pares con criterios de calidad (objetivo: aprobación en primera revisión)
Comunicación	Documentación técnica es clara, completa y accesible para audiencias técnicas y no técnicas	Evaluación de claridad de documentación por stakeholders (objetivo: 90% de comprensión)
Cohérence	Configuraciones de seguridad son consistentes en todos los entornos y componentes	Número de inconsistencias identificadas en auditorías (objetivo: cero inconsistencias)
Traçabilité	Todos los cambios de infraestructura son versionados, auditables y reversibles	Porcentaje de cambios con trazabilidad completa (objetivo: 100%)
Pertinence	Configuraciones de seguridad son apropiadas para el contexto y requisitos específicos de la aplicación	Validación de alineación entre configuraciones y requisitos de seguridad (objetivo: 100%)
Posture	Profesional demuestra rigor en aplicación de estándares de seguridad, responsabilidad en gestión de accesos y proactividad en identificación de vulnerabilidades	Evaluación de comportamientos de seguridad observados durante provisión (objetivo: comportamiento consistente)

Umbral de validación : Promedio ≥ 10/20

Bloque 3 - Automatización e Infraestructura como Código

Indicadores de desempeño por misión

Misión	Indicadores SMART
M05 — Gestionar software en la nube	Número de despliegues automatizados ejecutados sin intervención manual Tiempo medio de despliegue de aplicaciones (reducción porcentual) Tasa de éxito de despliegues automatizados (% sin rollback) Cobertura de automatización de tareas operativas repetitivas
M07 — Aplicar buenas prácticas de desarrollo seguro	Número de vulnerabilidades detectadas en análisis SAST/DAST antes de despliegue Tiempo medio de remediación de vulnerabilidades identificadas Porcentaje de despliegues bloqueados por fallos de seguridad Cobertura de análisis de dependencias vulnerables
M11 — Automatizar tareas de infraestructura cloud	Número de recursos cloud provistos mediante IaC (% de total) Tiempo de provisión de infraestructura (reducción porcentual) Consistencia de configuraciones entre entornos (% de conformidad) Número de cambios de infraestructura auditables y reversibles

Situaciones de evaluación

Despliegue Automatizado de Aplicación Containerizada en Kubernetes

Contexto : Una empresa necesita desplegar una aplicación microservicios en Kubernetes de forma automatizada y segura. La aplicación consta de 3 servicios independientes que deben escalarse automáticamente según carga. Se requiere integración de análisis de seguridad en el pipeline de despliegue y validación de configuraciones antes de despliegue en producción.

Restricciones : El despliegue debe completarse en menos de 10 minutos, sin intervención manual. Todas las imágenes de contenedor deben pasar análisis SAST/DAST. Las configuraciones de Kubernetes deben validarse contra políticas de seguridad. Debe existir capacidad de rollback automático en caso de fallo.

Producciones esperadas :

- Manifiestos Kubernetes (Deployments, Services, ConfigMaps, Secrets) versionados en repositorio Git
- Pipeline CI/CD automatizado con etapas de build, test, análisis de seguridad y despliegue
- Configuración de escalado automático (HPA) basado en métricas de CPU y memoria
- Documentación de procedimiento de despliegue y rollback
- Reporte de análisis de seguridad (SAST/DAST) con vulnerabilidades identificadas y remediadas

Competencias evaluadas : C7, C9, C11

Provisión de Infraestructura Cloud mediante Infrastructure as Code

Contexto : Una organización requiere provisionar un entorno cloud completo (redes, instancias, almacenamiento, bases de datos) de forma reproducible y versionada. El entorno debe ser idéntico en desarrollo, staging y producción. Se requiere validación de configuraciones de seguridad y auditoría de cambios.

Restricciones : Todo recurso cloud debe definirse en código IaC (Terraform o CloudFormation). Las configuraciones deben validarse antes de aplicarse. Debe existir historial completo de cambios en repositorio Git. Las credenciales y secretos no deben almacenarse en código. Debe ser posible destruir y recrear el entorno completo en menos de 30 minutos.

Producciones esperadas :

- Código IaC modular y reutilizable (módulos de Terraform o stacks de CloudFormation)
- Archivo de variables y configuración por entorno
- Validación de código IaC mediante herramientas de linting y análisis estático
- Documentación de arquitectura de infraestructura y decisiones de diseño
- Plan de cambios (terraform plan) revisado y aprobado antes de aplicación
- Auditoría de cambios de infraestructura con trazabilidad completa

Competencias evaluadas : C7, C9, C11

Implementación de Arquitectura de Mensajería Asíncrona para Desacoplamiento

Contexto : Una aplicación monolítica necesita desacoplarse mediante arquitectura de eventos. Se requiere implementar colas de mensajes y buses de eventos para comunicación asíncrona entre componentes. La solución debe garantizar entrega confiable de mensajes, manejo de errores y escalabilidad.

Restricciones : Debe utilizarse servicio de mensajería cloud (SQS/SNS, Service Bus, Pub/Sub). Todos los flujos de eventos deben documentarse con diagramas. Debe implementarse manejo de errores con dead-letter queues. Debe validarse integridad de datos en flujos de eventos. Debe monitorearse salud de colas y latencia de procesamiento.

Producciones esperadas :

- Diagrama de arquitectura de eventos con flujos de mensajes documentados
- Configuración de colas y tópicos de mensajería con políticas de retención
- Código de productores y consumidores de mensajes con manejo de errores
- Configuración de dead-letter queues y políticas de reintentos
- Validación de esquemas de mensajes (JSON Schema, Protobuf)
- Dashboards de monitoreo de colas con alertas de anomalías

Competencias evaluadas : C7, C9, C11

Integración de Análisis de Seguridad en Pipeline DevOps

Contexto : Una organización necesita integrar análisis de vulnerabilidades (SAST/DAST) en su pipeline de CI/CD para identificar y mitigar riesgos de seguridad tempranamente. Se requiere automatizar escaneo de código, dependencias y artefactos, bloqueando despliegues inseguros.

Restricciones : Análisis SAST debe ejecutarse en cada commit. Análisis DAST debe ejecutarse antes de despliegue en staging. Todas las vulnerabilidades críticas deben bloquear despliegue. Debe existir proceso de excepción documentado para vulnerabilidades aceptadas. Debe reportarse tendencia de vulnerabilidades.

Producciones esperadas :

- Configuración de herramientas SAST (SonarQube, Checkmarx) integradas en pipeline
- Configuración de herramientas DAST (OWASP ZAP, Burp Suite) para pruebas automatizadas
- Escaneo de dependencias vulnerables (SBOM) con identificación de librerías desactualizadas
- Políticas de gates de seguridad que bloquean despliegues inseguros
- Reportes de vulnerabilidades con severidad, impacto y recomendaciones de remediación
- Documentación de proceso de gestión de vulnerabilidades y excepciones

Competencias evaluadas : C7, C9, C11

Automatización de Tareas Operativas mediante Scripting

Contexto : Una organización requiere automatizar tareas operativas repetitivas (provisión de usuarios, rotación de credenciales, aplicación de parches, limpieza de recursos) mediante scripts reutilizables. Los scripts deben ser idempotentes, auditables y fáciles de mantener.

Restricciones : Scripts deben ser idempotentes (ejecutables múltiples veces sin efectos secundarios). Debe existir validación de precondiciones antes de ejecución. Todos los cambios deben ser auditables con logs detallados. Scripts deben incluir manejo de errores y rollback. Debe documentarse claramente propósito y uso de cada script.

Producciones esperadas :

- Scripts de automatización en Python/Bash con validación de entrada
- Playbooks de Ansible para tareas de configuración repetitivas
- Documentación de scripts con ejemplos de uso y casos de error
- Logs detallados de ejecución de scripts con trazabilidad de cambios
- Mecanismos de rollback para scripts que modifican estado
- Pruebas unitarias de scripts de automatización

Competencias evaluadas : C7, C9, C11

Pruebas esperadas

■ Pruebas documentales

- Código IaC versionado en repositorio Git con historial de cambios
- Manifiestos Kubernetes con configuraciones de seguridad validadas
- Configuración de pipelines CI/CD con etapas de análisis de seguridad
- Documentación de arquitectura de eventos y flujos de mensajería
- Reportes de análisis SAST/DAST con vulnerabilidades identificadas
- Políticas de seguridad en código IaC (validación de configuraciones)
- Documentación de procedimientos de despliegue y rollback
- Logs de auditoría de cambios de infraestructura
- Esquemas de validación de mensajes (JSON Schema, Protobuf)
- Documentación de scripts de automatización con ejemplos de uso

■ **Pruebas de acción (en campo)**

- Provisión de infraestructura cloud mediante Terraform/CloudFormation sin intervención manual
- Despliegue automatizado de aplicaciones en Kubernetes con validación de seguridad
- Ejecución de análisis SAST/DAST en pipeline CI/CD bloqueando despliegues inseguros
- Configuración de colas de mensajes y buses de eventos con manejo de errores
- Escalado automático de contenedores basado en métricas de carga
- Ejecución de scripts de automatización idempotentes con validación de precondiciones
- Rollback automático de despliegues fallidos
- Monitoreo de flujos de eventos y alertas de anomalías
- Validación de integridad de datos en migraciones automatizadas
- Aplicación de parches de seguridad mediante automatización

■ **Pruebas reflexivas**

- Análisis de causas raíz de fallos en despliegues automatizados
- Evaluación de efectividad de análisis de seguridad en identificación de vulnerabilidades
- Revisión de decisiones de diseño de arquitectura de eventos
- Análisis de impacto de cambios de infraestructura en rendimiento y costes
- Evaluación de cobertura de automatización y oportunidades de mejora
- Reflexión sobre trade-offs entre automatización y control manual
- Análisis de tendencias de vulnerabilidades identificadas en pipelines
- Evaluación de confiabilidad de flujos de mensajería
- Revisión de procedimientos de rollback y capacidad de recuperación
- Análisis de lecciones aprendidas en implementación de IaC

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Todas las configuraciones de infraestructura cumplen con estándares de seguridad (CIS Benchmarks, ISO 27001) validadas mediante herramientas de análisis	Porcentaje de configuraciones que pasan validación de cumplimiento de estándares de seguridad
Qualité	El código IaC es modular, reutilizable y sigue convenciones de nomenclatura consistentes, facilitando mantenimiento y escalabilidad	Número de módulos reutilizables creados, complejidad ciclomática del código IaC, cobertura de documentación
Comunicación	La documentación de arquitectura de automatización es clara y accesible para equipos técnicos y no técnicos, incluyendo diagramas y ejemplos	Completitud de documentación, claridad de explicaciones, número de ejemplos prácticos incluidos
Pertinence	Las soluciones de automatización resuelven problemas reales de operación, reducen intervención manual y mejoran eficiencia operativa	Reducción de tiempo de despliegue, reducción de errores manuales, cobertura de automatización de tareas repetitivas
Cohérence	Las decisiones de automatización son coherentes con arquitectura general, patrones de diseño y estándares organizacionales	Alineación con patrones arquitectónicos definidos, consistencia con estándares de codificación, integración con herramientas existentes

Familia	Definición	Ponderación
Traçabilité	Todos los cambios de infraestructura y despliegues son auditables, versionados y reversibles, con historial completo de cambios	Porcentaje de cambios con trazabilidad completa, capacidad de rollback, logs de auditoría disponibles
Posture	El profesional demuestra rigor en validación de automatización, responsabilidad operativa en monitoreo de despliegues y pensamiento en seguridad en pipelines	Número de validaciones realizadas antes de despliegue, tiempo de respuesta ante anomalías, vulnerabilidades detectadas en análisis de seguridad

Umbral de validación : Promedio ≥ 10/20

Bloque 4 - Operación, Monitoreo y Optimización de Servicios Cloud

Indicadores de desempeño por misión

Misión	Indicadores SMART
M03 — Monitorear el rendimiento de servicios cloud	Porcentaje de servicios cloud monitoreados con métricas de rendimiento (APM, trazas distribuidas) en tiempo real Cumplimiento de SLOs definidos: disponibilidad, latencia y tasa de error dentro de rangos aceptables Tiempo promedio de detección de anomalías desde su ocurrencia hasta identificación por sistema de monitoreo Número de incidentes prevenidos mediante análisis proactivo de tendencias de rendimiento
M04 — Gestionar servidores en la nube	Disponibilidad de servidores cloud monitoreados (uptime percentage) Tiempo promedio de respuesta a alertas de estado de servidores Cumplimiento de procedimientos de hardening en 100% de servidores nuevos Número de vulnerabilidades de configuración identificadas y remediadas mensualmente
M10 — Supervisar entornos cloud híbridos	Cobertura de monitoreo unificado en entornos híbridos (% de recursos monitoreados) Tiempo de respuesta a alertas en entornos híbridos (on-premises y cloud) Precisión de detección de anomalías en entornos híbridos (tasa de falsos positivos) Disponibilidad de dashboards unificados para visualización de estado de servicios

Situaciones de evaluación

Configuración de Monitoreo Integral de Servicios Cloud

Contexto : Una empresa ha desplegado una aplicación crítica en AWS con múltiples componentes (API, base de datos, colas de mensajes). Se requiere establecer monitoreo completo que garantice cumplimiento de SLOs de disponibilidad del 99.9% y latencia máxima de 200ms.

Restricciones : Presupuesto limitado para herramientas de monitoreo; necesidad de integración con sistemas de alertas existentes; requisito de retención de datos de 30 días.

Producciones esperadas :

- Configuración de CloudWatch/Azure Monitor con métricas de rendimiento (CPU, memoria, latencia, tasa de error)
- Definición de SLIs cuantificables (disponibilidad, latencia p99, tasa de error)
- Configuración de alertas con umbrales basados en SLOs
- Dashboard operativo mostrando estado de servicios y cumplimiento de SLOs
- Documentación de procedimientos de respuesta a alertas

Competencias evaluadas : C5

Análisis de Tendencias y Optimización de Costes

Contexto : Una organización opera infraestructura cloud en AWS con costes mensuales de $50,000. Se requiere identificar oportunidades de optimización mediante análisis de utilización de recursos y tendencias de carga.

Restricciones : Datos históricos limitados (3 meses); múltiples equipos con diferentes patrones de uso; necesidad de validar cambios sin impacto en rendimiento.

Producciones esperadas :

- Análisis de utilización de instancias EC2 identificando sobredimensionamiento
- Recomendaciones de rightsizing con estimación de ahorros
- Propuesta de estrategia de compra (instancias reservadas vs. spot instances)
- Desglose de costes por servicio y departamento
- Reportes de tendencias de costes con proyecciones futuras
- Plan de implementación de optimizaciones con validación de impacto

Competencias evaluadas : C16

Respuesta a Incidente de Degradación de Rendimiento

Contexto : Un servicio cloud experimenta degradación de rendimiento: latencia aumenta de 100ms a 500ms, tasa de error sube a 5%. Se requiere investigación rápida, identificación de causa raíz y restauración de servicio.

Restricciones : Tiempo crítico (SLA en riesgo); múltiples componentes involucrados; necesidad de comunicación continua a stakeholders.

Producciones esperadas :

- Investigación sistemática utilizando logs, métricas y trazas distribuidas
- Identificación de causa raíz (ej: base de datos sobrecargada, fuga de memoria)
- Acciones correctivas inmediatas para restaurar servicio
- Validación de recuperación de métricas a valores normales
- Comunicación de estado a stakeholders durante incidente
- Post-mortem documentando lecciones aprendidas y mejoras preventivas

Competencias evaluadas : C5

Monitoreo de Entorno Cloud Híbrido

Contexto : Una empresa opera aplicaciones en cloud pública (AWS) y on-premises. Se requiere establecer monitoreo unificado que proporcione visibilidad completa del estado de servicios en ambos entornos.

Restricciones : Herramientas heterogéneas en ambos entornos; latencia de red entre entornos; requisito de correlación de eventos entre múltiples fuentes.

Producciones esperadas :

- Configuración de agentes de monitoreo en ambos entornos
- Integración de datos de monitoreo en plataforma centralizada
- Dashboards unificados mostrando estado de servicios on-premises y cloud
- Alertas correlacionadas que detectan problemas en cualquier entorno
- Análisis de anomalías en entorno híbrido
- Documentación de arquitectura de monitoreo híbrido

Competencias evaluadas : C5

Validación de Cumplimiento de SLAs y Mejora Continua

Contexto : Se requiere evaluar cumplimiento de SLAs de servicios cloud durante los últimos 3 meses, identificar causas de incumplimientos y proponer mejoras de resiliencia.

Restricciones : Datos de monitoreo incompletos en algunos períodos; múltiples servicios con diferentes SLOs; necesidad de validar mejoras sin afectar operaciones.

Producciones esperadas :

- Cálculo de cumplimiento de SLAs por servicio y período
- Análisis de incidentes que causaron incumplimiento de SLAs
- Identificación de patrones de fallos recurrentes
- Propuestas de mejoras de resiliencia (redundancia, escalado automático)
- Validación de mejoras mediante simulacros de fallo
- Reportes de cumplimiento y mejoras a stakeholders
- Documentación de lecciones aprendidas

Competencias evaluadas : C5

Pruebas esperadas

■ Pruebas documentales

- Configuración de herramientas de monitoreo (CloudWatch, Datadog, Prometheus) exportada y documentada
- Definición de SLIs y SLOs en documento técnico con justificación de valores
- Dashboards operativos capturados mostrando métricas de rendimiento en tiempo real
- Reportes de análisis de tendencias con gráficos históricos y proyecciones
- Análisis de costes con desglose por servicio, proyecto y departamento
- Recomendaciones de optimización documentadas con estimación de ahorros
- Runbooks de respuesta a incidentes con procedimientos paso a paso
- Reportes de cumplimiento de SLAs con cálculos detallados
- Post-mortems de incidentes documentando causa raíz y lecciones aprendidas
- Documentación de arquitectura de monitoreo híbrido con diagramas

■ Pruebas de acción (en campo)

- Configuración de alertas en herramientas de monitoreo con umbrales basados en SLOs
- Creación de dashboards operativos personalizados mostrando métricas críticas
- Implementación de rightsizing de instancias con validación de impacto en rendimiento
- Ejecución de análisis de costes identificando oportunidades de ahorro
- Respuesta a incidentes de rendimiento investigando causa raíz y restaurando servicio
- Escalado automático de recursos basado en métricas de carga
- Implementación de mejoras de resiliencia (redundancia, failover automático)
- Ejecución de simulacros de fallo para validar planes de recuperación
- Comunicación de estado de servicios a stakeholders durante incidentes
- Revisión periódica de configuración de monitoreo y ajuste de alertas

■ Pruebas reflexivas

- Análisis de efectividad de alertas: ¿detectan problemas antes de afectar usuarios?
- Evaluación de precisión de SLOs: ¿son realistas y alineados con expectativas de negocio?
- Reflexión sobre causas raíz de incidentes: ¿qué patrones se repiten?
- Análisis de impacto de optimizaciones de costes: ¿se mantiene rendimiento y disponibilidad?
- Evaluación de cobertura de monitoreo: ¿hay puntos ciegos en visibilidad?

• Reflexión sobre mejoras de resiliencia: ¿son suficientes para cumplir SLOs?
• Análisis de tendencias de carga: ¿se anticipan cambios futuros correctamente?
• Evaluación de comunicación durante incidentes: ¿se informó a stakeholders adecuadamente?
• Reflexión sobre automatización de respuestas: ¿se pueden automatizar más acciones?
• Análisis de lecciones aprendidas: ¿se implementan mejoras preventivas?

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Configuración de monitoreo cumple con estándares de observabilidad (métricas, logs, trazas distribuidas) y requisitos de retención de datos	100% de servicios críticos monitoreados con al menos 3 pilares de observabilidad; retención de datos según política
Qualité	Métricas de rendimiento son precisas, actualizadas en tiempo real y correlacionadas correctamente entre componentes	Latencia de reporte de métricas < 1 minuto; precisión de métricas validada contra logs de aplicación
Comunicación	Alertas comunican claramente problemas de rendimiento con contexto suficiente para investigación rápida	Tiempo promedio de investigación de alerta < 15 minutos; 90% de alertas contienen información de contexto
Pertinence	SLOs definidos son realistas, alineados con requisitos de negocio y validados mediante datos históricos	SLOs cumplidos en 95%+ de períodos; feedback positivo de stakeholders sobre realismo de objetivos
Cohérence	Estrategia de optimización de costes es coherente con requisitos de rendimiento y disponibilidad	Ahorros de costes logrados sin degradación de SLOs; validación de impacto en rendimiento antes de implementación
Traçabilité	Todos los cambios de configuración de monitoreo y optimización están documentados y auditables	100% de cambios registrados en sistema de control de versiones; auditoría de cambios disponible
Posture	Profesional demuestra proactividad en detección de problemas, disciplina en cumplimiento de SLAs y orientación a mejora continua	Problemas detectados antes de afectar usuarios en 80%+ de casos; propuestas de mejora documentadas regularmente

Umbral de validación : Promedio ≥ 10/20

Bloque 5 - Gestión de Servidores, Software y Contenedores

Indicadores de desempeño por misión

Misión	Indicadores SMART
M04 — Gestionar servidores en la nube	Porcentaje de instancias cloud provisionadas mediante IaC con versionado completo Tiempo medio de provisión de instancias desde solicitud hasta disponibilidad Número de vulnerabilidades de hardening identificadas y remediadas en ciclo de auditoría Disponibilidad promedio de instancias monitoreadas (uptime %)
M05 — Gestionar software en la nube	Número de despliegues de contenedores ejecutados exitosamente sin incidentes Tiempo medio de escalado automático desde detección de carga hasta disponibilidad de recursos Porcentaje de aplicaciones con monitoreo de salud (liveness/readiness probes) configurado Tasa de rollback automático exitoso ante fallos de despliegue
M11 — Automatizar tareas de infraestructura cloud	Porcentaje de tareas de infraestructura automatizadas mediante IaC Tiempo ahorrado mensualmente mediante automatización de tareas repetitivas Número de cambios de infraestructura ejecutados sin intervención manual Tasa de éxito de despliegues automatizados (sin errores de configuración)

Situaciones de evaluación

Provisión y Hardening de Instancias Cloud en Entorno Productivo

Contexto : Un equipo de DevOps debe provisionar un conjunto de instancias cloud (AWS EC2, Azure VMs o GCP Compute Engine) para alojar una aplicación web crítica. Las instancias deben cumplir con estándares de seguridad (CIS Benchmarks), estar monitoreadas continuamente y ser gestionadas mediante Infrastructure as Code.

Restricciones : Las instancias deben estar disponibles en menos de 30 minutos, cumplir con políticas de seguridad corporativas, tener configurados grupos de seguridad restrictivos, y estar completamente documentadas en código IaC versionado.

Producciones esperadas :

- Código Terraform/CloudFormation/Pulumi que provisiona instancias con configuración segura
- Playbooks de Ansible o Chef que aplican hardening a instancias
- Configuración de grupos de seguridad y reglas de firewall
- Dashboards de monitoreo de estado y rendimiento de instancias
- Documentación de configuración de seguridad aplicada

Competencias evaluadas : C6

Despliegue y Escalado Automático de Aplicaciones en Kubernetes

Contexto : Un equipo debe desplegar una aplicación containerizada en un cluster Kubernetes en cloud (EKS, AKS o GKE), configurar escalado automático basado en métricas de CPU y memoria, y garantizar que la aplicación se recupere automáticamente ante fallos de pods.

Restricciones : El despliegue debe ser reproducible mediante manifiestos YAML, el escalado debe responder en menos de 2 minutos a cambios de carga, y debe implementarse una estrategia de despliegue rolling sin downtime.

Producciones esperadas :

- Manifiestos YAML de Kubernetes (Deployments, Services, ConfigMaps, HPA)
- Configuración de Horizontal Pod Autoscaler con métricas personalizadas
- Liveness y readiness probes para monitoreo de salud de pods
- Estrategia de despliegue rolling con validación de integridad
- Documentación de procedimientos de escalado y rollback

Competencias evaluadas : C7

Implementación de Arquitectura Asíncrona con Mensajería Cloud

Contexto : Un equipo debe diseñar e implementar una arquitectura asíncrona utilizando servicios de mensajería cloud (AWS SQS/SNS, Azure Service Bus, GCP Pub/Sub o Kafka) para desacoplar componentes de una aplicación distribuida y mejorar escalabilidad.

Restricciones : La solución debe garantizar entrega de mensajes al menos una vez, implementar manejo de errores con dead-letter queues, y validar integridad de datos en flujos de mensajes. El monitoreo debe detectar anomalías en menos de 5 minutos.

Producciones esperadas :

- Configuración de colas y tópicos de mensajería
- Código de productores y consumidores de mensajes
- Políticas de reintentos y manejo de errores
- Configuración de dead-letter queues y alertas
- Dashboards de monitoreo de flujos de mensajes
- Documentación de patrones de mensajería implementados

Competencias evaluadas : C11

Automatización de Gestión de Ciclo de Vida de Software en Cloud

Contexto : Un equipo DevOps debe automatizar el despliegue, actualización y monitoreo de aplicaciones en instancias cloud utilizando herramientas de gestión de configuración (Ansible, Chef, Puppet) e Infrastructure as Code, garantizando consistencia y trazabilidad.

Restricciones : Todos los cambios deben ser versionados en repositorio Git, las actualizaciones deben ejecutarse sin downtime, y debe existir capacidad de rollback automático ante fallos. El proceso debe ser completamente automatizado sin intervención manual.

Producciones esperadas :

- Playbooks de Ansible o recetas de Chef para despliegue de aplicaciones
- Código IaC que define infraestructura y configuración de software
- Pipelines CI/CD que automatizan despliegue y validación
- Procedimientos de rollback automático
- Monitoreo de integridad de despliegues
- Documentación de procedimientos de automatización

Competencias evaluadas : C6, C7

Auditoría de Seguridad y Hardening de Componentes Cloud

Contexto : Un equipo de seguridad debe realizar auditoría de seguridad de instancias y contenedores en producción, identificar desviaciones de configuración segura, aplicar hardening según CIS Benchmarks, y validar cumplimiento de políticas de seguridad corporativas.

Restricciones : La auditoría debe completarse sin interrumpir servicios, los hallazgos deben documentarse con severidad y recomendaciones, y el hardening debe validarse mediante escaneo automatizado antes de aplicación en producción.

Producciones esperadas :

- Reporte de auditoría de seguridad con hallazgos y severidades
- Playbooks de Ansible para remediación de vulnerabilidades
- Configuración de políticas de seguridad en grupos de seguridad
- Validación de cumplimiento de CIS Benchmarks
- Dashboards de monitoreo de postura de seguridad
- Plan de remediación con cronograma

Competencias evaluadas : C6

Pruebas esperadas

■ Pruebas documentales

- Código IaC versionado en repositorio Git con historial de cambios
- Manifiestos YAML de Kubernetes con anotaciones de decisiones de diseño
- Playbooks de Ansible o recetas de Chef documentados con comentarios
- Configuración de herramientas de monitoreo (Prometheus, Grafana, CloudWatch)
- Reportes de auditoría de seguridad con hallazgos y recomendaciones
- Documentación de procedimientos operativos (runbooks) para gestión de componentes
- Políticas de escalado automático documentadas con justificación de umbrales
- Registros de cambios de configuración con trazabilidad completa

■ Pruebas de acción (en campo)

- Provisión de instancias cloud mediante IaC sin intervención manual
- Aplicación de hardening a instancias mediante playbooks automatizados
- Despliegue de aplicaciones en Kubernetes con validación de integridad
- Escalado automático de pods en respuesta a cambios de carga
- Implementación de colas de mensajes y validación de flujos
- Ejecución de auditorías de seguridad y remediación de vulnerabilidades
- Monitoreo continuo de estado y rendimiento de componentes
- Rollback automático de despliegues ante fallos detectados

■ Pruebas reflexivas

- Análisis de decisiones de arquitectura de componentes y justificación de alternativas
- Evaluación de efectividad de estrategias de escalado automático
- Reflexión sobre lecciones aprendidas en despliegues fallidos
- Análisis de impacto de cambios de configuración en rendimiento y seguridad
- Evaluación de cobertura de monitoreo y alertas
- Análisis de tendencias de utilización de recursos y oportunidades de optimización
- Reflexión sobre mejoras en procedimientos operativos basadas en incidentes
- Evaluación de efectividad de herramientas de automatización utilizadas

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Todas las instancias y contenedores cumplen con estándares de seguridad (CIS Benchmarks, ISO 27001) validados mediante escaneo automatizado	Porcentaje de componentes que pasan validación de cumplimiento de seguridad (objetivo: 100%)
Qualité	Las configuraciones de componentes son reproducibles, versionadas y documentadas en código IaC sin errores de sintaxis	Número de despliegues exitosos sin errores de configuración / total de despliegues (objetivo: ≥95%)
Comunicación	La documentación de componentes es clara, completa y accesible para equipos técnicos y operativos	Evaluación de claridad y completitud de documentación por pares (escala 1-5, objetivo: ≥4)
Cohérence	Los componentes están correctamente integrados en arquitectura general, con dependencias claramente documentadas	Número de incidentes causados por desalineación de componentes / total de incidentes (objetivo: 0%)
Traçabilité	Todos los cambios de configuración están versionados, auditados y trazables a decisiones de negocio	Porcentaje de cambios con registro de auditoría completo (objetivo: 100%)
Pertinence	Las decisiones de gestión de componentes están alineadas con requisitos de rendimiento, disponibilidad y costes	Cumplimiento de SLOs de disponibilidad y rendimiento (objetivo: ≥99.5%)
Posture	El profesional demuestra responsabilidad en mantenimiento de componentes, proactividad en identificación de problemas y orientación a automatización	Evaluación de comportamientos profesionales por supervisores y pares (escala 1-5, objetivo: ≥4)

Umbral de validación : Promedio ≥ 10/20

Bloque 6 - Integración de Sistemas y Arquitecturas de Mensajería

Indicadores de desempeño por misión

Misión	Indicadores SMART
M06 — Integrar soluciones cloud con sistemas existentes	Número de sistemas heredados integrados exitosamente con cloud sin pérdida de datos Tiempo promedio de latencia en flujos de integración síncrona (objetivo: <500ms) Porcentaje de mensajes procesados correctamente en colas asíncronas (objetivo: >99.9%) Número de incidentes de integración resueltos en menos de 1 hora
M13 — Realizar seguimiento de proyectos cloud	Porcentaje de hitos de proyecto completados dentro del cronograma planificado Número de desviaciones de proyecto identificadas y comunicadas a stakeholders Tiempo promedio de resolución de problemas de integración reportados Satisfacción de stakeholders con comunicación de estado del proyecto (escala 1-5)

Situaciones de evaluación

Diseño e Implementación de Integración Síncrona con API REST

Contexto : Una empresa tiene un sistema heredado de gestión de pedidos on-premises que debe integrarse con una solución de facturación en AWS. El sistema heredado expone datos mediante una API SOAP antigua, y la solución cloud requiere integración mediante REST. Se necesita garantizar latencia baja (<500ms) y manejo robusto de errores.

Restricciones : La API heredada tiene limitaciones de throughput (máximo 100 llamadas/segundo). No se puede modificar el sistema heredado. Se requiere versionado de API para compatibilidad hacia atrás. Debe implementarse en menos de 2 semanas.

Producciones esperadas :

- Especificación técnica de API REST con esquema OpenAPI
- Código de adaptador que transforma SOAP a REST
- Configuración de circuit breaker y reintentos
- Documentación de contrato de API con ejemplos
- Plan de pruebas de integración

Competencias evaluadas : C8, C11, C18

Arquitectura de Mensajería Asíncrona para Desacoplamiento de Componentes

Contexto : Una plataforma de e-commerce en cloud necesita procesar pedidos de forma asíncrona. Los pedidos llegan a través de una API, deben procesarse en múltiples sistemas (inventario, facturación, envíos) de forma independiente. Se requiere garantizar que cada pedido se procesa exactamente una vez, incluso ante fallos.

Restricciones : El volumen de pedidos puede variar de 100 a 10,000 por hora. Algunos sistemas de procesamiento pueden estar temporalmente no disponibles. Se requiere auditoría completa de todos los pedidos procesados. Presupuesto limitado para servicios cloud.

Producciones esperadas :

- Diagrama de arquitectura de mensajería con colas y tópicos
- Configuración de colas de mensajes (SQS/Service Bus) con políticas de retención
- Implementación de dead letter queues para manejo de errores
- Código de consumidor de mensajes con idempotencia
- Documentación de garantías de entrega y manejo de fallos

Competencias evaluadas : C8, C11

Integración de Sistema Heredado con Arquitectura Cloud Híbrida

Contexto : Una organización financiera necesita integrar su sistema de gestión de riesgos on-premises (que no puede migrarse por requisitos regulatorios) con nuevos servicios analíticos en cloud. El sistema heredado procesa datos sensibles y requiere conectividad segura. Se necesita sincronizar datos diariamente con validación de integridad.

Restricciones : Conectividad limitada entre on-premises y cloud (VPN con ancho de banda limitado). El sistema heredado solo soporta transferencia de archivos (SFTP). Requisitos de cumplimiento normativo estrictos (auditoría completa). Datos sensibles requieren cifrado en tránsito y en reposo.

Producciones esperadas :

- Diagrama de arquitectura híbrida con componentes de integración
- Especificación de flujo de sincronización de datos
- Configuración de VPN y conectividad segura
- Procedimiento de validación de integridad de datos
- Plan de recuperación ante fallos de conectividad
- Documentación de cumplimiento normativo

Competencias evaluadas : C8, C18

Coordinación de Proyecto de Integración Multi-Equipo

Contexto : Se inicia un proyecto de integración que requiere coordinación entre: equipo de sistemas heredados (3 personas), equipo cloud (4 personas), equipo de seguridad (2 personas) y stakeholders de negocio. El proyecto tiene duración de 3 meses con múltiples fases de integración. Se requiere comunicación clara de dependencias y riesgos.

Restricciones : Equipos distribuidos en diferentes zonas horarias. Cambios frecuentes en requisitos de negocio. Limitaciones técnicas del sistema heredado descubiertas durante el proyecto. Presión de negocio para acelerar entrega.

Producciones esperadas :

- Plan de proyecto detallado con fases, hitos y cronograma
- Matriz de responsabilidades (RACI) entre equipos
- Registro de riesgos con planes de mitigación
- Reportes de estado semanales para stakeholders
- Documentación de decisiones y cambios de alcance
- Plan de comunicación y escalamiento

Competencias evaluadas : C18

Validación y Pruebas de Integridad en Flujos de Integración

Contexto : Después de implementar una integración entre sistema heredado y cloud, se requiere validar que todos los datos se han transferido correctamente, sin pérdidas ni duplicados. Se necesitan pruebas exhaustivas de escenarios de fallo (desconexión de red, timeout, datos corruptos) para garantizar robustez.

Restricciones : Datos de prueba limitados (no se puede usar datos de producción). Ventanas de prueba limitadas en sistema heredado. Requisitos de auditoría requieren trazabilidad completa. Se requieren pruebas de carga para validar rendimiento.

Producciones esperadas :

- Plan de pruebas de integración detallado
- Casos de prueba para escenarios normales y de fallo
- Datos de prueba representativos
- Procedimiento de validación de integridad de datos
- Reporte de resultados de pruebas
- Documentación de problemas encontrados y resoluciones

Competencias evaluadas : C8, C11, C18

Pruebas esperadas

■ Pruebas documentales

- Especificación técnica de API con esquema OpenAPI o WSDL
- Diagramas de flujo de integración (secuencia, datos)
- Documentación de patrones de integración seleccionados
- Configuración de servicios de mensajería (colas, tópicos, políticas)
- Procedimientos operativos (runbooks) de integración
- Documentación de decisiones arquitectónicas (ADRs) de integración
- Planes de proyecto con cronograma y asignación de recursos
- Reportes de estado de proyecto
- Documentación de validación de integridad de datos
- Procedimientos de recuperación ante fallos

■ Pruebas de acción (en campo)

- Implementación de adaptadores de integración (SOAP a REST, transformación de datos)
- Configuración de colas de mensajes y tópicos en servicios cloud
- Implementación de circuit breaker y reintentos en código
- Despliegue de integraciones en entornos de staging y producción
- Ejecución de pruebas de integración end-to-end
- Validación de integridad de datos en flujos de integración
- Monitoreo de flujos de integración en producción
- Coordinación de equipos en reuniones de proyecto
- Resolución de problemas de integración en tiempo real
- Implementación de mejoras basadas en lecciones aprendidas

■ Pruebas reflexivas

- Análisis de trade-offs entre patrones de integración síncrona vs asíncrona
- Evaluación de decisiones de selección de servicios de mensajería
- Reflexión sobre lecciones aprendidas en integraciones anteriores
- Análisis de impacto de cambios en requisitos de integración
- Evaluación de efectividad de procedimientos de recuperación ante fallos
- Análisis de comunicación y coordinación entre equipos
- Reflexión sobre mejoras en procesos de integración
- Evaluación de cumplimiento de SLAs de integración
- Análisis de costes de diferentes opciones de integración
- Reflexión sobre escalabilidad de soluciones de integración

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Las integraciones cumplen con estándares de seguridad (cifrado en tránsito y en reposo, autenticación, autorización) y requisitos regulatorios (auditoría, trazabilidad)	100% de integraciones implementadas con controles de seguridad validados; auditoría completa de cambios de datos
Qualité	Los flujos de integración funcionan correctamente sin pérdida de datos, con latencia aceptable y manejo robusto de errores	Tasa de éxito de integración >99.9%; latencia <500ms para síncronos; 0 pérdidas de datos en validaciones
Comunicación	La documentación de integraciones es clara y completa; la comunicación entre equipos es efectiva y oportuna	Documentación técnica completa con diagramas y ejemplos; reportes de estado semanales; 100% de decisiones documentadas
Cohérence	Las soluciones de integración son coherentes con arquitectura cloud general y patrones organizacionales	Alineación con patrones arquitectónicos definidos; reutilización de componentes de integración; consistencia en decisiones
Traçabilité	Todos los flujos de integración son trazables, con logging completo y auditoría de cambios de datos	Logs detallados de todos los eventos de integración; auditoría completa de transformaciones de datos; trazabilidad de errores

Familia	Definición	Ponderación
Pertinence	Las soluciones de integración responden a requisitos de negocio y técnicos identificados	100% de requisitos de integración implementados; validación de requisitos por stakeholders; cumplimiento de criterios de éxito
Posture	El profesional demuestra rigor en validación, responsabilidad en coordinación y orientación a confiabilidad de integraciones	Validación exhaustiva de integraciones antes de producción; comunicación proactiva de riesgos; mejora continua de procesos

Umbral de validación : Promedio ≥ 10/20

Bloque 7 - Seguridad Cloud y Cumplimiento Normativo

Indicadores de desempeño por misión

Misión	Indicadores SMART
M02 — Configurar entornos cloud públicos	Porcentaje de configuraciones de seguridad que cumplen con CIS Benchmarks (objetivo: 100%) Número de vulnerabilidades críticas identificadas y remediadas en menos de 48 horas Cobertura de controles de seguridad en todos los servicios cloud provistos (objetivo: 100%) Tiempo medio de detección de desviaciones de configuración de seguridad (objetivo: < 1 hora)
M07 — Aplicar buenas prácticas de desarrollo seguro	Número de vulnerabilidades detectadas en análisis SAST/DAST antes de despliegue Porcentaje de dependencias con vulnerabilidades conocidas identificadas (objetivo: 100%) Tiempo de remediación promedio de vulnerabilidades críticas (objetivo: < 24 horas) Cobertura de análisis de seguridad en pipeline CI/CD (objetivo: 100% de cambios)
M15 — Evaluar soluciones de infraestructura en la nube	Cumplimiento de requisitos normativos evaluados (RGPD, SOC 2, PCI-DSS, etc.) Número de certificaciones de seguridad obtenidas por proveedores evaluados Porcentaje de requisitos de cumplimiento mapeados a controles técnicos Tiempo de evaluación de cumplimiento normativo de proveedores (objetivo: < 2 semanas)

Situaciones de evaluación

Evaluación de Postura de Seguridad en Entorno Cloud Existente

Contexto : Una organización ha desplegado servicios en AWS durante 6 meses. Se requiere evaluar la postura de seguridad actual, identificar desviaciones de estándares (CIS Benchmarks, ISO 27001) y proponer plan de remediación. El profesional debe analizar configuraciones de seguridad, políticas IAM, cifrado, logging y controles de acceso.

Restricciones : Evaluación sin interrumpir servicios en producción. Acceso limitado a ciertos recursos. Requisito de documentación exhaustiva de hallazgos. Plazo de 2 semanas para evaluación completa.

Producciones esperadas :

- Informe de evaluación de postura de seguridad con hallazgos clasificados por severidad
- Matriz de mapeo de requisitos de estándares (CIS, ISO 27001) a controles implementados
- Plan de remediación priorizado con cronograma de implementación
- Recomendaciones de mejora de configuración de seguridad
- Documentación de configuraciones de seguridad validadas

Competencias evaluadas : C4, C15, C23

Implementación de Controles de Seguridad en Nuevo Entorno Cloud

Contexto : Se está provisioning un nuevo entorno cloud en Azure para aplicación crítica que procesa datos personales (RGPD). El profesional debe configurar controles de seguridad completos: cifrado, gestión de identidades, segmentación de red, logging, auditoría y cumplimiento normativo. Debe garantizar que todas las configuraciones cumplan con RGPD y estándares de seguridad.

Restricciones : Cumplimiento obligatorio de RGPD. Validación de configuraciones antes de despliegue. Documentación de todas las decisiones de seguridad. Coordinación con equipo de cumplimiento normativo. Plazo de 4 semanas.

Producciones esperadas :

- Configuración de controles de seguridad en Azure (cifrado, IAM, NSG, logging)
- Políticas IAM con principio de mínimo privilegio documentadas
- Matriz de responsabilidad compartida completada
- Documentación de cumplimiento RGPD
- Plan de auditoría y monitoreo de seguridad
- Validación de configuraciones contra CIS Benchmarks

Competencias evaluadas : C4, C15, C24

Integración de Análisis de Vulnerabilidades en Pipeline DevOps

Contexto : Equipo de desarrollo necesita integrar análisis de seguridad (SAST/DAST) en pipeline CI/CD existente. El profesional debe configurar herramientas de análisis, definir políticas de bloqueo de despliegues inseguros, establecer proceso de remediación de vulnerabilidades y capacitar al equipo en prácticas DevSecOps.

Restricciones : No debe ralentizar significativamente pipeline (máximo 10% de aumento de tiempo). Debe permitir despliegues rápidos de parches de seguridad. Integración con herramientas existentes (Jenkins, GitLab CI). Documentación clara de políticas de seguridad.

Producciones esperadas :

- Configuración de herramientas SAST/DAST en pipeline
- Políticas de bloqueo de despliegues inseguros
- Proceso de remediación de vulnerabilidades documentado
- Reportes de análisis de vulnerabilidades automatizados
- Documentación de prácticas DevSecOps para equipo
- Métricas de vulnerabilidades detectadas y remediadas

Competencias evaluadas : C9, C23

Auditoría de Cumplimiento Normativo y Certificación de Seguridad

Contexto : Organización requiere obtener certificación SOC 2 Type II para cumplir requisitos de clientes. El profesional debe evaluar cumplimiento actual, identificar brechas, implementar controles faltantes y coordinar auditoría externa. Debe documentar evidencia de cumplimiento y mantener registros de auditoría.

Restricciones : Auditoría externa programada en 3 meses. Requisito de evidencia documentada de todos los controles. Coordinación con múltiples departamentos. Cumplimiento de requisitos de retención de logs.

Producciones esperadas :

- Matriz de mapeo de requisitos SOC 2 a controles implementados
- Documentación de políticas y procedimientos de seguridad
- Evidencia de implementación de controles (logs, configuraciones, reportes)
- Plan de remediación de brechas identificadas
- Reportes de auditoría interna
- Documentación de cambios de seguridad y auditoría

Competencias evaluadas : C4, C15, C24

Respuesta a Incidente de Seguridad y Análisis Post-Incidente

Contexto : Se detecta acceso no autorizado a recursos cloud. El profesional debe investigar incidente, contener amenaza, remediar vulnerabilidad explotada, documentar hallazgos y proponer mejoras preventivas. Debe coordinar con equipo de seguridad y comunicar a stakeholders.

Restricciones : Respuesta inmediata requerida. Minimizar impacto en servicios. Preservar evidencia forense. Documentación completa del incidente. Comunicación clara a stakeholders.

Producciones esperadas :

- Informe de investigación de incidente con cronología de eventos
- Análisis de causa raíz del incidente
- Acciones de contención y remediación ejecutadas
- Recomendaciones de mejora preventiva
- Actualización de políticas de seguridad
- Comunicación a stakeholders sobre incidente y acciones tomadas

Competencias evaluadas : C4, C15, C23

Pruebas esperadas

■ Pruebas documentales

- Informe de evaluación de postura de seguridad con hallazgos clasificados por severidad
- Matriz de mapeo de requisitos de estándares de seguridad (CIS Benchmarks, ISO 27001, SOC 2) a controles implementados
- Políticas de seguridad documentadas (gestión de accesos, cifrado, logging, auditoría)
- Configuraciones de seguridad validadas (código IaC, manifiestos cloud)
- Documentación de cumplimiento normativo (RGPD, LOPD-GDD, PCI-DSS, SOC 2)
- Planes de remediación de vulnerabilidades con cronograma
- Reportes de análisis de vulnerabilidades (SAST/DAST)
- Registros de auditoría de accesos y eventos de seguridad
- Documentación de incidentes de seguridad e investigaciones
- Certificaciones de seguridad obtenidas (SOC 2, ISO 27001, etc.)
- Procedimientos operativos estándar (SOPs) de seguridad
- Matriz de responsabilidad compartida completada

■ Pruebas de acción (en campo)

- Configurar controles de seguridad en servicios cloud (cifrado, IAM, segmentación de red, logging)
- Implementar políticas IAM con principio de mínimo privilegio
- Ejecutar escaneo de vulnerabilidades y análisis de postura de seguridad
- Integrar herramientas SAST/DAST en pipeline CI/CD
- Investigar y responder a incidentes de seguridad
- Remediar vulnerabilidades identificadas en plazo establecido
- Realizar auditorías de cumplimiento normativo
- Implementar controles de seguridad faltantes
- Revocar accesos innecesarios y validar principio de mínimo privilegio
- Monitorear eventos de seguridad y alertas de anomalías
- Ejecutar simulacros de respuesta a incidentes
- Validar configuraciones de seguridad contra estándares

■ Pruebas reflexivas

- Análisis de efectividad de controles de seguridad implementados

- Evaluación de cobertura de controles de seguridad en todos los servicios
- Reflexión sobre lecciones aprendidas de incidentes de seguridad
- Análisis de tendencias de vulnerabilidades y amenazas
- Evaluación de alineación de controles con requisitos normativos
- Análisis de impacto de cambios de seguridad en operaciones
- Reflexión sobre mejoras en cultura de seguridad del equipo
- Evaluación de eficiencia de procesos de remediación de vulnerabilidades
- Análisis de brechas entre estándares de seguridad y prácticas actuales
- Reflexión sobre comunicación de riesgos de seguridad a stakeholders

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Todas las configuraciones de seguridad cumplen con estándares aplicables (CIS Benchmarks, ISO 27001, SOC 2, RGPD)	Porcentaje de configuraciones que pasan validación contra estándares (objetivo: 100%)
Qualité	Controles de seguridad están completamente implementados, documentados y validados antes de despliegue en producción	Número de vulnerabilidades críticas encontradas en auditoría post-despliegue (objetivo: 0)
Comunicación	Riesgos de seguridad se comunican claramente a stakeholders técnicos y de negocio con impacto cuantificado	Porcentaje de stakeholders que comprenden riesgos comunicados (evaluación mediante encuesta)
Pertinence	Controles de seguridad seleccionados son relevantes para amenazas identificadas y requisitos normativos aplicables	Cobertura de amenazas identificadas por controles implementados (objetivo: 100%)
Cohérence	Controles de seguridad están integrados coherentemente en arquitectura cloud sin crear conflictos o redundancias innecesarias	Número de conflictos o redundancias identificadas en revisión de arquitectura de seguridad (objetivo: 0)
Traçabilité	Todos los cambios de seguridad, accesos y eventos están registrados y auditables para cumplimiento normativo	Porcentaje de eventos de seguridad registrados en logs de auditoría (objetivo: 100%)
Posture	Profesional demuestra vigilancia continua, responsabilidad en aplicación de controles y liderazgo en cultura de seguridad	Evaluación de comportamientos de seguridad por supervisores y pares (escala 1-5)

Umbral de validación : Promedio ≥ 10/20

Bloque 8 - Almacenamiento, Datos y Bases de Datos Cloud

Indicadores de desempeño por misión

Misión	Indicadores SMART
M01 — Diseñar arquitecturas cloud escalables	Número de patrones arquitectónicos de almacenamiento identificados y documentados en el diseño Porcentaje de requisitos de escalabilidad de datos cubiertos por la arquitectura propuesta Tiempo de respuesta de consultas en la arquitectura diseñada (latencia en milisegundos) Coste estimado de almacenamiento anual según la arquitectura propuesta
M13 — Realizar seguimiento de proyectos cloud	Porcentaje de datos migrados exitosamente sin pérdida de integridad Tiempo total de migración de datos (horas/días) Número de validaciones de integridad realizadas y aprobadas Desviación de cronograma de migración respecto al plan original (porcentaje)
M14 — Definir estrategias de adopción de cloud	Número de opciones de bases de datos evaluadas y comparadas Porcentaje de requisitos de cumplimiento normativo cubiertos por la solución seleccionada Coste total de propiedad (TCO) estimado para la solución de datos Tiempo de implementación estimado de la solución de datos

Situaciones de evaluación

Diseño de Solución de Almacenamiento para Aplicación de E-commerce

Contexto : Una empresa de e-commerce necesita diseñar una solución de almacenamiento cloud para gestionar catálogos de productos, imágenes de alta resolución, datos de transacciones y logs de auditoría. La solución debe soportar crecimiento de 100% anual, garantizar disponibilidad del 99.99%, cumplir con GDPR y optimizar costes.

Restricciones : Presupuesto limitado para almacenamiento, requisito de latencia baja para acceso a catálogos, necesidad de retención de datos de 7 años para auditoría, restricciones de residencia de datos en UE.

Producciones esperadas :

- Diagrama de arquitectura de almacenamiento mostrando tipos de almacenamiento seleccionados
- Matriz de comparación de opciones de almacenamiento (objeto, bloque, archivo)
- Especificación de políticas de ciclo de vida de datos
- Estimación de costes anuales de almacenamiento
- Documento de cumplimiento normativo (GDPR, residencia de datos)

Competencias evaluadas : C1, C13, C31

Migración de Base de Datos Heredada a Cloud

Contexto : Una organización financiera necesita migrar una base de datos Oracle de 2TB con datos críticos de clientes a Azure SQL Database. La migración debe completarse en 48 horas con cero downtime, garantizar integridad de datos y cumplir con PCI-DSS.

Restricciones : Ventana de migración limitada a fin de semana, requisito de validación exhaustiva de datos, necesidad de rollback rápido si hay problemas, cifrado obligatorio de datos sensibles.

Producciones esperadas :

- Plan detallado de migración con fases y cronograma
- Script de validación de integridad de datos
- Documentación de estrategia de cifrado y seguridad
- Reporte de reconciliación de datos post-migración
- Procedimiento de rollback documentado

Competencias evaluadas : C13, C4, C15

Optimización de Costes de Almacenamiento en Entorno Multi-Cloud

Contexto : Una empresa con presencia en AWS, Azure y GCP necesita optimizar costes de almacenamiento que actualmente representan el 35% del presupuesto cloud. Existen datos con diferentes patrones de acceso: frecuente, ocasional y archivos.

Restricciones : No se puede comprometer el rendimiento de aplicaciones críticas, necesidad de mantener redundancia geográfica, requisito de auditoría de cambios de almacenamiento.

Producciones esperadas :

- Análisis detallado de utilización actual de almacenamiento por tipo y proveedor
- Recomendaciones de optimización con estimación de ahorros
- Propuesta de reclasificación de datos a clases de almacenamiento económicas
- Plan de implementación de políticas de ciclo de vida
- Proyección de costes anuales post-optimización

Competencias evaluadas : C1, C13, C31

Implementación de Arquitectura de Data Lake en Cloud

Contexto : Una empresa de análisis necesita construir un data lake en AWS para consolidar datos de múltiples fuentes (APIs, bases de datos, archivos). El data lake debe soportar análisis en tiempo real, machine learning y cumplir con gobernanza de datos.

Restricciones : Datos provenientes de fuentes heterogéneas con diferentes formatos, requisito de catalogación automática de datos, necesidad de control de calidad de datos, presupuesto limitado para procesamiento.

Producciones esperadas :

- Arquitectura de data lake con capas (raw, processed, curated)
- Especificación de pipelines ETL/ELT
- Configuración de catálogo de datos y metadatos
- Políticas de gobernanza y calidad de datos
- Estimación de costes de almacenamiento y procesamiento

Competencias evaluadas : C1, C13, C31

Evaluación y Selección de Base de Datos Gestionada para Aplicación de IoT

Contexto : Una empresa de IoT necesita seleccionar una base de datos gestionada en cloud para almacenar millones de eventos de sensores diarios. La solución debe soportar escritura de alta velocidad, consultas analíticas y escalado automático.

Restricciones : Requisito de latencia baja (< 100ms), necesidad de retención de datos de 5 años, presupuesto limitado para bases de datos, cumplimiento con regulaciones de privacidad.

Producciones esperadas :

- Matriz de evaluación de opciones de bases de datos (relacional, NoSQL, series temporales)
- Análisis técnico de cada opción (escalabilidad, rendimiento, costo)
- Recomendación justificada con trade-offs
- Especificación de configuración de la base de datos seleccionada
- Plan de migración de datos históricos

Competencias evaluadas : C1, C13, C31

Pruebas esperadas

■ Pruebas documentales

- Diagramas de arquitectura de almacenamiento con notación clara
- Especificaciones técnicas de soluciones de almacenamiento
- Planes de migración de datos documentados
- Políticas de ciclo de vida de datos
- Matrices de evaluación de opciones de almacenamiento
- Reportes de validación de integridad de datos
- Documentación de cumplimiento normativo
- Estimaciones de costes de almacenamiento
- Procedimientos de backup y recuperación
- Catálogos de datos y metadatos

■ Pruebas de acción (en campo)

- Provisión de servicios de almacenamiento cloud (S3, Blob Storage, GCS)
- Configuración de políticas de ciclo de vida de datos
- Implementación de cifrado en almacenamiento
- Ejecución de migraciones de datos con validación
- Configuración de réplicas y redundancia
- Implementación de controles de acceso a datos
- Monitoreo de utilización de almacenamiento
- Optimización de costes mediante reclasificación de datos
- Ejecución de pruebas de recuperación de datos
- Implementación de pipelines de datos

■ Pruebas reflexivas

- Análisis de trade-offs entre rendimiento y coste de almacenamiento
- Evaluación de impacto de decisiones de arquitectura de datos en escalabilidad
- Reflexión sobre lecciones aprendidas en migraciones de datos
- Análisis de efectividad de políticas de ciclo de vida implementadas
- Evaluación de cumplimiento normativo en soluciones de almacenamiento
- Análisis de optimizaciones de costes logradas
- Reflexión sobre mejoras en gobernanza de datos

• Evaluación de integridad de datos post-migración
• Análisis de rendimiento de bases de datos gestionadas
• Reflexión sobre mejora continua en gestión de datos

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	La solución de almacenamiento cumple con todos los requisitos regulatorios identificados (GDPR, HIPAA, PCI-DSS, residencia de datos)	Checklist de cumplimiento normativo completado al 100%
Qualité	La integridad de datos se valida exhaustivamente mediante reconciliación, checksums y auditoría post-migración	Porcentaje de registros validados exitosamente (≥99.99%)
Comunicación	Las decisiones de arquitectura de almacenamiento se documentan claramente con justificación de trade-offs y alternativas evaluadas	Documentación técnica completa con diagramas y especificaciones detalladas
Pertinence	La solución de almacenamiento se alinea con requisitos técnicos y empresariales identificados (escalabilidad, rendimiento, coste)	Cobertura de requisitos: ≥95% de requisitos funcionales y no funcionales cubiertos
Cohérence	La arquitectura de datos es coherente con patrones arquitectónicos modernos y mejores prácticas de cloud	Validación de coherencia arquitectónica mediante revisión de pares
Traçabilité	Todos los cambios de almacenamiento y datos se registran, auditan y pueden ser rastreados para cumplimiento y recuperación	Logs de auditoría completos con trazabilidad de cambios al 100%
Posture	El profesional demuestra rigor en validación de datos, responsabilidad en seguridad y orientación a optimización de costes	Evaluación de comportamientos profesionales mediante observación de prácticas aplicadas

Umbral de validación : Promedio ≥ 10/20

Bloque 9 - Continuidad, Recuperación y Copias de Seguridad

Indicadores de desempeño por misión

Misión	Indicadores SMART
M09 — Asegurar la continuidad de los servicios cloud	Porcentaje de servicios críticos con planes BCP/DRP documentados y validados Cumplimiento de RTO y RPO definidos en simulacros de recuperación Número de brechas identificadas y cerradas en planes de recuperación Tiempo promedio de ejecución de procedimientos de recuperación en simulacros
M04 — Gestionar servidores en la nube	Frecuencia de ejecución de backups automatizados sin fallos Porcentaje de backups validados exitosamente en pruebas de restauración Tiempo promedio de restauración de instancias desde backup Cumplimiento de políticas de retención de backups
M03 — Monitorear el rendimiento de servicios cloud	Disponibilidad de servicios monitoreados versus SLO definido Tiempo de detección de fallos de backup o replicación Precisión de alertas de estado de recuperación Cobertura de monitoreo de componentes críticos de recuperación

Situaciones de evaluación

Diseño de Plan de Continuidad de Negocio para Aplicación Crítica

Contexto : Una empresa de servicios financieros requiere diseñar un plan de continuidad de negocio para su aplicación de procesamiento de pagos. La aplicación actual se ejecuta en una única región cloud y procesa 10,000 transacciones diarias. Se requiere definir RTO de 4 horas y RPO de 1 hora para cumplir con requisitos regulatorios.

Restricciones : Presupuesto limitado para infraestructura redundante, requisitos de cumplimiento normativo (PCI-DSS), latencia máxima aceptable de 100ms para transacciones

Producciones esperadas :

- Documento de Plan de Continuidad de Negocio con análisis de impacto empresarial
- Definición clara de RTO y RPO con justificación técnica
- Arquitectura de recuperación con replicación entre regiones
- Procedimientos de failover y comunicación durante desastres
- Matriz de criticidad de servicios y componentes

Competencias evaluadas : C14

Implementación de Estrategia de Copias de Seguridad Automatizadas

Contexto : Un equipo de operaciones cloud necesita implementar una estrategia de copias de seguridad para 50 instancias de base de datos y 200 máquinas virtuales distribuidas en múltiples regiones cloud. Se requiere automatización completa, validación de integridad y cumplimiento de políticas de retención según regulación GDPR.

Restricciones : Optimización de costes de almacenamiento, validación automática de restauración, cumplimiento de regulaciones de privacidad de datos

Producciones esperadas :

- Política de copias de seguridad documentada con tipos, frecuencia y retención
- Configuración de servicios de backup cloud (AWS Backup, Azure Backup o equivalente)
- Scripts de automatización de backups con validación de integridad
- Procedimientos de restauración granular y completa
- Reportes de cumplimiento de políticas de backup

Competencias evaluadas : C34

Ejecución de Simulacro de Recuperación ante Desastres

Contexto : Una organización debe ejecutar un simulacro completo de recuperación ante desastres para validar su plan DRP. El simulacro incluye failover de aplicaciones críticas a una región alterno, restauración de datos desde backups y validación de funcionalidad. Se espera completar la recuperación dentro del RTO definido de 2 horas.

Restricciones : Minimizar impacto en servicios en producción, validar cumplimiento de RTO/RPO, documentar todos los pasos y resultados

Producciones esperadas :

- Plan detallado del simulacro con cronograma y responsabilidades
- Registro de ejecución del simulacro con timestamps
- Validación de cumplimiento de RTO y RPO
- Identificación de debilidades y brechas en el plan
- Informe de lecciones aprendidas con recomendaciones de mejora

Competencias evaluadas : C35

Validación de Integridad de Datos Post-Restauración

Contexto : Después de una restauración de datos desde backup, se requiere validar exhaustivamente la integridad de datos en una base de datos crítica con 500 GB de información. Se deben reconciliar datos entre el sistema original y el restaurado, identificar discrepancias y documentar el proceso de validación.

Restricciones : Minimizar tiempo de validación, garantizar exactitud de reconciliación, cumplir con requisitos de auditoría

Producciones esperadas :

- Procedimiento de validación de integridad documentado
- Scripts de reconciliación de datos
- Reporte de validación con resultados de checksums
- Identificación y resolución de discrepancias
- Certificación de integridad de datos restaurados

Competencias evaluadas : C34, C35

Mejora Continua de Plan de Recuperación basada en Resultados de Simulacro

Contexto : Basándose en los resultados de un simulacro de recuperación, se identificaron varias debilidades: procedimientos desactualizados, falta de claridad en roles, y tiempo de recuperación superior al RTO. Se requiere analizar los hallazgos, actualizar el plan y comunicar mejoras a los equipos.

Restricciones : Incorporar feedback de múltiples equipos, validar mejoras en próximo simulacro, documentar cambios realizados

Producciones esperadas :

- Análisis detallado de resultados del simulacro
- Identificación de causas raíz de debilidades
- Plan de mejora con acciones correctivas priorizadas
- Procedimientos actualizados y clarificados
- Comunicación de cambios a equipos y stakeholders

Competencias evaluadas : C14, C35

Pruebas esperadas

■ Pruebas documentales

- Plan de Continuidad de Negocio (BCP) documentado con análisis de impacto empresarial
- Plan de Recuperación ante Desastres (DRP) con procedimientos detallados
- Definición de RTO y RPO con justificación técnica y empresarial
- Política de copias de seguridad con tipos, frecuencia y retención
- Configuración de servicios de backup cloud versionada en repositorio
- Procedimientos de restauración granular y completa documentados
- Matriz de criticidad de servicios y componentes
- Registros de simulacros de recuperación con resultados y timestamps
- Reportes de validación de integridad de datos
- Informe de lecciones aprendidas con recomendaciones de mejora
- Documentación de cambios en planes de recuperación
- Certificaciones de cumplimiento normativo en recuperación

■ Pruebas de acción (en campo)

- Configurar replicación de datos entre regiones cloud
- Implementar backups automatizados con validación de integridad
- Ejecutar simulacro completo de recuperación ante desastres
- Restaurar datos desde backup en entorno aislado
- Validar integridad de datos restaurados mediante checksums
- Ejecutar procedimientos de failover automático
- Documentar y comunicar resultados de simulacro a equipos
- Actualizar procedimientos basados en hallazgos de simulacro
- Implementar mejoras identificadas en plan de recuperación
- Monitorear estado de backups y replicación en tiempo real
- Ejecutar pruebas de restauración granular de datos específicos
- Validar cumplimiento de RTO y RPO en simulacros

■ Pruebas reflexivas

- Análisis de efectividad de estrategia de backup implementada
- Reflexión sobre debilidades identificadas en simulacro de recuperación
- Evaluación de cumplimiento de RTO y RPO en escenarios reales

• Análisis de impacto de mejoras implementadas en resiliencia
• Reflexión sobre capacidad de respuesta del equipo ante incidentes
• Evaluación de claridad y completitud de procedimientos de recuperación
• Análisis de lecciones aprendidas de simulacros anteriores
• Reflexión sobre alineación de planes de recuperación con objetivos empresariales
• Evaluación de efectividad de comunicación durante incidentes
• Análisis de mejoras continuas en cultura de resiliencia organizativa

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Los planes de continuidad y recuperación cumplen con marcos de referencia reconocidos (ISO 22301, NIST) y regulaciones aplicables (GDPR, PCI-DSS, HIPAA)	Auditoría de conformidad con estándares, validación de cumplimiento normativo en documentación
Qualité	Los planes de recuperación son exhaustivos, detallados y validados regularmente mediante simulacros que demuestran capacidad de recuperación	Cobertura de componentes críticos en planes, frecuencia de simulacros, cumplimiento de RTO/RPO en pruebas
Comunicación	Los procedimientos de recuperación están documentados de forma clara y accesible, y se comunican efectivamente a equipos y stakeholders	Claridad de procedimientos, comprensión de equipos, efectividad de comunicación durante incidentes
Cohérence	Los planes de continuidad y recuperación están alineados con objetivos empresariales, requisitos regulatorios y arquitectura técnica	Alineación de RTO/RPO con requisitos empresariales, consistencia entre BCP y DRP, validación de arquitectura
Traçabilité	Todos los cambios en planes de recuperación, backups y procedimientos están documentados, versionados y auditables	Registro de cambios en repositorio, auditoría de acceso a backups, trazabilidad de restauraciones
Pertinence	Las estrategias de backup y recuperación son apropiadas para criticidad de servicios, volumen de datos y requisitos de disponibilidad	Alineación de estrategias con matriz de criticidad, validación de suficiencia de RTO/RPO, análisis de costes-beneficio
Posture	El profesional demuestra rigor en planificación de recuperación, responsabilidad en protección de datos, capacidad de respuesta ante crisis y orientación a mejora continua	Exhaustividad de planes, consistencia en ejecución de procedimientos, análisis de resultados de simulacros, implementación de mejoras

Umbral de validación : Promedio ≥ 10/20

Bloque 10 - Migración de Aplicaciones y Adopción Cloud

Indicadores de desempeño por misión

Misión	Indicadores SMART
M14 — Definir estrategias de adopción de cloud	Porcentaje de aplicaciones evaluadas para migración con análisis de dependencias completado Número de estrategias de migración identificadas y documentadas por aplicación Cumplimiento del cronograma de definición de estrategia de adopción cloud Alineación de KPIs de migración con objetivos empresariales cuantificados
M13 — Realizar seguimiento de proyectos cloud	Desviaciones de cronograma identificadas y comunicadas dentro de 24 horas Porcentaje de hitos de proyecto completados según cronograma Número de reportes de estado entregados a tiempo a stakeholders Tasa de resolución de riesgos identificados
M03 — Monitorear el rendimiento de servicios cloud	Porcentaje de aplicaciones migradas con monitoreo de rendimiento configurado Cumplimiento de SLOs post-migración medido en porcentaje Tiempo promedio de detección de anomalías post-migración Número de métricas de rendimiento comparadas pre y post-migración
M12 — Documentar configuraciones de arquitectura cloud	Número de planes de migración documentados con fases y cronograma Completitud de documentación de decisiones de migración (ADRs) Número de runbooks operativos creados para procedimientos post-migración Accesibilidad de documentación a equipos técnicos y de negocio

Situaciones de evaluación

Análisis y Planificación de Migración de Aplicación Empresarial

Contexto : Una empresa de servicios financieros necesita migrar una aplicación monolítica crítica de 10 años de antigüedad desde infraestructura on-premises a cloud pública. La aplicación tiene múltiples dependencias con sistemas heredados, requisitos de cumplimiento normativo estrictos (PCI-DSS, GDPR) y debe mantener disponibilidad 24/7 durante la migración.

Restricciones : Tiempo máximo de planificación: 4 semanas. Disponibilidad de equipos técnicos limitada. Requisitos de seguridad y cumplimiento no negociables. Presupuesto de migración definido.

Producciones esperadas :

- Análisis detallado de dependencias de aplicación con mapeo de componentes
- Evaluación de tres estrategias de migración (rehost, replatform, refactor) con matriz de comparación
- Plan de migración con fases, cronograma, hitos y asignación de recursos
- Identificación de riesgos técnicos y empresariales con estrategias de mitigación
- Documento de alineación de migración con objetivos empresariales y KPIs

Competencias evaluadas : C12, C18, C20

Ejecución y Coordinación de Migración Multi-Fase

Contexto : Coordinación de migración de cartera de 15 aplicaciones a cloud en 6 meses. Equipos distribuidos geográficamente, múltiples proveedores cloud (AWS y Azure), requisitos de sincronización de datos complejos y necesidad de mantener operaciones en paralelo durante transición.

Restricciones : Cronograma fijo de 6 meses. Equipos con diferentes niveles de experiencia cloud. Necesidad de minimizar impacto en operaciones. Comunicación asincrónica entre equipos.

Producciones esperadas :

- Plan de proyecto detallado con fases, dependencias y cronograma de Gantt
- Matriz de riesgos con identificación, evaluación e impacto de riesgos
- Reportes de estado semanales a stakeholders con desviaciones y acciones correctivas
- Documentación de decisiones de migración (ADRs) para cada aplicación
- Procedimientos de escalado para problemas críticos

Competencias evaluadas : C18, C19

Validación de Rendimiento y Cumplimiento de SLAs Post-Migración

Contexto : Validación de 5 aplicaciones migradas a cloud para verificar que cumplen SLOs definidos. Aplicaciones incluyen servicios web, procesamiento de datos y bases de datos. Necesidad de comparar rendimiento pre y post-migración, identificar degradación y optimizar configuraciones.

Restricciones : Período de validación: 2 semanas post-migración. Acceso limitado a datos históricos pre-migración. Necesidad de mantener aplicaciones en producción durante validación. Herramientas de monitoreo limitadas inicialmente.

Producciones esperadas :

- Configuración de dashboards de monitoreo con métricas clave (latencia, throughput, disponibilidad)
- Informe comparativo de rendimiento pre y post-migración con análisis de desviaciones
- Validación de cumplimiento de SLOs con documentación de resultados
- Identificación de problemas de rendimiento con recomendaciones de optimización
- Plan de mejora continua basado en análisis de métricas

Competencias evaluadas : C5, C12

Liderazgo de Transformación Organizativa y Adopción Cloud

Contexto : Liderazgo de programa de transformación cloud en organización de 200 personas con resistencia al cambio. Necesidad de capacitar equipos en nuevas prácticas, promover adopción de cloud, cambiar cultura organizativa y asegurar transferencia de conocimiento de sistemas heredados.

Restricciones : Presupuesto de formación limitado. Equipos con experiencia limitada en cloud. Necesidad de mantener operaciones durante transformación. Tiempo disponible para capacitación limitado.

Producciones esperadas :

- Programa de capacitación diseñado con módulos, cronograma y recursos
- Documentación de procedimientos operativos en cloud (runbooks)
- Plan de comunicación de cambios con mensajes clave y canales
- Métricas de adopción cloud con seguimiento de progreso
- Programa de mentoría para profesionales en transición

Competencias evaluadas : C19, C20

Gestión de Migración de Datos Críticos con Validación de Integridad

Contexto : Migración de base de datos crítica de 500 GB con datos financieros sensibles desde on-premises a cloud. Requisitos de integridad de datos estrictos, necesidad de validación completa, minimización de downtime y cumplimiento de regulaciones de privacidad.

Restricciones : Ventana de migración: 4 horas. Datos en constante cambio. Herramientas de validación limitadas. Requisitos de auditoría estrictos.

Producciones esperadas :

- Plan de migración de datos con estrategia de sincronización y validación
- Scripts de validación de integridad de datos pre y post-migración
- Documentación de procedimientos de rollback
- Informe de validación de integridad de datos con reconciliación completa
- Procedimientos de monitoreo post-migración de datos

Competencias evaluadas : C12, C13

Pruebas esperadas

■ Pruebas documentales

- Plan de migración documentado con fases, cronograma y asignación de recursos
- Análisis de dependencias de aplicaciones con mapeo de componentes
- Matriz de evaluación de estrategias de migración (rehost, replatform, refactor)
- Documento de alineación de migración con objetivos empresariales y KPIs
- Matriz de riesgos con identificación, evaluación e impacto
- Reportes de estado de proyecto con desviaciones y acciones correctivas
- Decisiones arquitectónicas (ADRs) documentadas para migraciones
- Runbooks operativos para procedimientos post-migración
- Informe comparativo de rendimiento pre y post-migración
- Validación de cumplimiento de SLOs post-migración
- Programa de capacitación con módulos y cronograma
- Plan de comunicación de cambios con mensajes clave
- Scripts de validación de integridad de datos
- Procedimientos de rollback documentados

■ Pruebas de acción (en campo)

- Análisis exhaustivo de dependencias de aplicaciones identificando componentes críticos
- Evaluación de tres estrategias de migración con matriz de comparación
- Planificación de fases de migración con cronograma y hitos
- Identificación y evaluación de riesgos técnicos y empresariales
- Coordinación de equipos distribuidos en ejecución de migración
- Monitoreo de cronograma y gestión de desviaciones
- Comunicación de estado a stakeholders con escalado de problemas
- Configuración de monitoreo de rendimiento post-migración
- Validación de cumplimiento de SLOs con análisis de métricas
- Identificación de problemas de rendimiento y optimización
- Ejecución de migración de datos con validación de integridad
- Liderazgo de programa de capacitación en cloud
- Promoción de adopción de cloud en equipos
- Facilitación de transferencia de conocimiento

■ Pruebas reflexivas

- Reflexión sobre decisiones de estrategia de migración y trade-offs evaluados
- Análisis de lecciones aprendidas en planificación de migraciones
- Evaluación de efectividad de plan de migración versus ejecución real
- Análisis de riesgos materializados y efectividad de mitigaciones
- Reflexión sobre comunicación con stakeholders y gestión de expectativas
- Análisis de desviaciones de cronograma y causas raíz
- Evaluación de validación de rendimiento post-migración
- Reflexión sobre cumplimiento de SLOs y oportunidades de optimización
- Análisis de efectividad de programa de capacitación
- Evaluación de adopción de cloud en equipos
- Reflexión sobre resistencia al cambio y estrategias de superación
- Análisis de integridad de datos post-migración
- Evaluación de alineación de migración con objetivos empresariales
- Reflexión sobre mejoras continuas en procesos de migración

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Pertinence	Las estrategias de migración seleccionadas se alinean claramente con requisitos técnicos y empresariales de la aplicación	Matriz de evaluación de estrategias documenta alineación con requisitos; stakeholders validan pertinencia de estrategia seleccionada
Conformité	El plan de migración cumple con requisitos de seguridad, cumplimiento normativo y políticas organizativas	Auditoría de plan de migración verifica cumplimiento de estándares de seguridad (CIS, ISO 27001); validación de requisitos regulatorios (PCI-DSS, GDPR)
Qualité	La ejecución de migración mantiene integridad de datos, funcionalidad de aplicaciones y rendimiento equivalente o mejorado	Validación de integridad de datos post-migración con reconciliación completa; pruebas de funcionalidad con 100% de casos de uso validados; comparación de métricas de rendimiento pre y post-migración
Cohérence	El plan de migración es coherente con arquitectura cloud objetivo y decisiones arquitectónicas documentadas	ADRs documentan decisiones de migración; plan de migración referencia decisiones arquitectónicas; validación de alineación entre plan y arquitectura
Traçabilité	Todas las decisiones, cambios y resultados de migración están documentados y auditables	Documentación completa de decisiones (ADRs); registro de cambios de configuración; logs de ejecución de migración; reportes de validación

Familia	Definición	Ponderación
Comunicación	La comunicación con stakeholders es clara, oportuna y mantiene expectativas alineadas durante migración	Reportes de estado entregados según cronograma; desviaciones comunicadas dentro de 24 horas; feedback de stakeholders indica claridad de comunicación
Posture	El profesional demuestra liderazgo en adopción de cloud, promueve cambio cultural y facilita transferencia de conocimiento	Programa de capacitación completado con participación de equipos; métricas de adopción cloud muestran progreso; feedback de equipos indica liderazgo efectivo

Umbral de validación : Promedio ≥ 10/20

Bloque 11 - Optimización de Costes y Recursos Cloud

Indicadores de desempeño por misión

Misión	Indicadores SMART
M02 — Configurar entornos cloud públicos	Porcentaje de reducción de costes de infraestructura cloud mediante optimización de instancias Número de instancias sobredimensionadas identificadas y redimensionadas Ahorro económico anual logrado mediante estrategias de compra (instancias reservadas, spot) Tiempo promedio de identificación de anomalías de costes
M14 — Definir estrategias de adopción de cloud	Costo total de propiedad (TCO) estimado vs. realizado en adopción cloud Retorno de inversión (ROI) de proyectos cloud Alineación de costes reales con presupuesto planificado Número de oportunidades de optimización identificadas en estrategia de adopción
M15 — Evaluar soluciones de infraestructura en la nube	Diferencia de costes entre proveedores cloud evaluados Análisis de costo-beneficio de soluciones cloud vs. on-premises Identificación de costes ocultos en evaluación de proveedores Precisión de proyecciones de costes en evaluación de soluciones

Situaciones de evaluación

Análisis de Rightsizing de Instancias Cloud

Contexto : Una organización opera 150 instancias EC2 en AWS con patrones de utilización variables. El equipo de operaciones necesita identificar oportunidades de optimización de costes sin comprometer rendimiento de aplicaciones críticas. Se requiere analizar datos de utilización de CPU y memoria de los últimos 3 meses, identificar instancias sobredimensionadas y proponer cambios de tipo de instancia con estimación de ahorro.

Restricciones : Análisis basado en datos reales de CloudWatch; validación de impacto en rendimiento mediante pruebas; documentación de recomendaciones con justificación económica; comunicación clara de riesgos y beneficios.

Producciones esperadas :

- Informe de análisis de utilización de instancias con métricas de CPU, memoria y red
- Matriz de recomendaciones de rightsizing con tipo de instancia actual, propuesto y ahorro estimado
- Análisis de impacto en rendimiento de cambios propuestos
- Plan de implementación con cronograma y validación de cambios
- Estimación de ahorro económico anual

Competencias evaluadas : C16, C2

Evaluación de Estrategias de Compra de Instancias Reservadas

Contexto : Una empresa necesita optimizar costes de infraestructura cloud evaluando opciones de compra (bajo demanda, instancias reservadas, spot instances, savings plans). Se requiere analizar patrones de carga de aplicaciones, evaluar opciones de compra disponibles en AWS/Azure/GCP, y recomendar estrategia óptima considerando flexibilidad y ahorro económico.

Restricciones : Análisis de patrones de carga de al menos 6 meses; evaluación de múltiples opciones de compra; consideración de trade-offs entre ahorro y flexibilidad; validación de recomendaciones con datos de costes reales.

Producciones esperadas :

- Análisis de patrones de carga identificando cargas predecibles y variables
- Comparativa de opciones de compra (bajo demanda, reservadas, spot, savings plans) con costes estimados
- Recomendación de estrategia óptima con justificación económica
- Análisis de ahorro potencial anual
- Plan de implementación de estrategia recomendada

Competencias evaluadas : C16, C2, C25

Análisis de Costes y Detección de Anomalías

Contexto : Una organización experimenta incremento inesperado de costes cloud del 35% en el último mes. Se requiere analizar datos de costes detalladamente, identificar causas del incremento, detectar anomalías y proponer acciones correctivas. Se debe utilizar herramientas de análisis de costes (AWS Cost Explorer, Azure Cost Management) y generar reportes para stakeholders.

Restricciones : Análisis granular de costes por servicio, proyecto y departamento; identificación de causas raíz del incremento; validación de datos de costes; comunicación clara de hallazgos a stakeholders técnicos y de negocio.

Producciones esperadas :

- Análisis detallado de costes por servicio, proyecto y departamento
- Identificación de causas del incremento de costes
- Detección de anomalías y patrones inusuales
- Reporte ejecutivo con hallazgos principales
- Recomendaciones de acciones correctivas con impacto económico estimado

Competencias evaluadas : C16, C25

Evaluación Económica de Proveedores Cloud

Contexto : Una empresa evalúa migración de aplicaciones a cloud y necesita comparar opciones de proveedores (AWS, Azure, GCP). Se requiere realizar análisis económico comparativo considerando modelos de precios, descuentos por volumen, costes de migración y costes de salida. Se debe evaluar también alineación con requisitos técnicos y cumplimiento normativo.

Restricciones : Análisis de múltiples proveedores; consideración de modelos de precios complejos; evaluación de costes totales de propiedad (TCO); análisis de costes de migración y salida; comunicación clara de trade-offs económicos.

Producciones esperadas :

- Análisis de modelos de precios de proveedores evaluados
- Comparativa de costes totales de propiedad (TCO) por proveedor
- Análisis de costes de migración y salida
- Evaluación de descuentos por volumen y opciones de compra
- Recomendación de proveedor con justificación económica y técnica

Competencias evaluadas : C2, C16

Implementación de Políticas de Gobernanza de Costes

Contexto : Una organización necesita implementar gobernanza de costes cloud para controlar gastos y asegurar alineación con presupuestos. Se requiere definir políticas de control de costes, establecer etiquetado de recursos, configurar alertas de presupuesto, y crear reportes de costes por proyecto y departamento. Se debe capacitar a equipos en prácticas de optimización de costes.

Restricciones : Definición de políticas claras y aplicables; implementación de etiquetado consistente; configuración de alertas y límites de presupuesto; creación de reportes automatizados; capacitación de equipos en gobernanza de costes.

Producciones esperadas :

- Políticas de control de costes documentadas
- Esquema de etiquetado de recursos definido e implementado
- Alertas de presupuesto configuradas por proyecto y departamento
- Reportes automatizados de costes por proyecto, departamento y servicio
- Programa de capacitación en gobernanza de costes para equipos

Competencias evaluadas : C16, C25

Pruebas esperadas

■ Pruebas documentales

- Informes de análisis de rightsizing con métricas de utilización y recomendaciones
- Análisis comparativo de opciones de compra (reservadas, spot, savings plans)
- Reportes de costes por servicio, proyecto y departamento
- Análisis de anomalías de costes con identificación de causas raíz
- Evaluación económica de proveedores cloud con análisis de TCO
- Políticas de gobernanza de costes documentadas
- Esquemas de etiquetado de recursos
- Planes de implementación de optimización con estimaciones de ahorro
- Reportes ejecutivos de costes para stakeholders
- Documentación de mejores prácticas de optimización

■ Pruebas de acción (en campo)

- Implementación de cambios de rightsizing en instancias cloud
- Compra de instancias reservadas basada en análisis de patrones de carga
- Configuración de alertas de presupuesto y límites de costes
- Implementación de políticas de etiquetado de recursos
- Automatización de reportes de costes
- Ejecución de simulacros de optimización de costes
- Validación de impacto de cambios de optimización en rendimiento
- Comunicación de resultados de optimización a stakeholders
- Implementación de políticas de ciclo de vida de datos
- Configuración de herramientas de análisis de costes

■ Pruebas reflexivas

- Análisis de efectividad de estrategias de optimización implementadas
- Evaluación de precisión de proyecciones de ahorro vs. resultados reales
- Reflexión sobre trade-offs entre ahorro y flexibilidad operativa
- Análisis de impacto de cambios de optimización en rendimiento de aplicaciones
- Evaluación de adopción de políticas de gobernanza de costes por equipos

- Análisis de lecciones aprendidas en proyectos de optimización
- Reflexión sobre mejora continua de procesos de optimización
- Evaluación de comunicación de costes a stakeholders
- Análisis de alineación de costes reales con presupuestos planificados
- Reflexión sobre evolución de cultura de optimización de costes

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	Las recomendaciones de optimización cumplen con políticas de gobernanza de costes y requisitos de presupuesto establecidos	100% de recomendaciones alineadas con políticas; presupuesto respetado en implementación
Qualité	El análisis de costes es exhaustivo, preciso y basado en datos reales de utilización y precios	Precisión de análisis >= 95%; cobertura de al menos 90% de recursos evaluados
Comunicación	Las recomendaciones de optimización se comunican claramente a stakeholders técnicos y de negocio con justificación económica	Reportes comprensibles para audiencias técnicas y no técnicas; impacto económico cuantificado
Pertinence	Las oportunidades de optimización identificadas son relevantes y viables de implementar sin comprometer rendimiento	Al menos 80% de recomendaciones implementadas; impacto en rendimiento <= 5%
Cohérence	Las estrategias de optimización son coherentes con arquitectura cloud y objetivos empresariales	Alineación de recomendaciones con arquitectura; ROI positivo de cambios implementados
Traçabilité	Todos los análisis, decisiones y cambios de optimización están documentados y trazables	100% de análisis documentados; auditoría completa de cambios implementados
Posture	El profesional demuestra orientación a eficiencia económica, rigor en análisis y responsabilidad en validación de cambios	Identificación proactiva de oportunidades; validación exhaustiva de impacto; comunicación clara de resultados

Umbral de validación : Promedio >= 10/20

Bloque 12 - Gestión de Proyectos, Documentación y Comunicación Cloud

Indicadores de desempeño por misión

Misión	Indicadores SMART
M12 — Documentar configuraciones de arquitectura cloud	Número de ADRs documentados con contexto, alternativas y consecuencias claramente registradas Cobertura de documentación técnica: porcentaje de componentes arquitectónicos documentados Completitud de runbooks operativos: número de procedimientos operativos documentados con pasos claros Actualización de documentación: frecuencia de revisión y actualización de documentación técnica
M13 — Realizar seguimiento de proyectos cloud	Cumplimiento de cronograma: porcentaje de hitos completados en fecha Gestión de desviaciones: tiempo promedio de identificación y escalado de problemas Comunicación de estado: frecuencia y completitud de reportes a stakeholders Satisfacción de stakeholders: evaluación de claridad y oportunidad de comunicación
M14 — Definir estrategias de adopción de cloud	Alineación de soluciones: porcentaje de requisitos empresariales traducidos a especificaciones técnicas Adopción de cloud: porcentaje de equipos capacitados en nuevas prácticas Cumplimiento de KPIs: logro de objetivos empresariales definidos Retorno de inversión: comparación de beneficios realizados vs. proyectados

Situaciones de evaluación

Documentación de Decisiones Arquitectónicas en Proyecto Cloud

Contexto : Un equipo de arquitectura cloud debe documentar decisiones clave tomadas durante el diseño de una solución de migración a cloud. Se requiere crear ADRs (Architecture Decision Records) que registren decisiones sobre selección de servicios, patrones arquitectónicos y estrategias de seguridad. Los ADRs deben ser comprensibles para arquitectos, desarrolladores y stakeholders de negocio.

Restricciones : Los ADRs deben seguir un formato estándar, incluir contexto claro, alternativas evaluadas, decisión tomada y consecuencias. Deben estar versionados en repositorio de control de versiones. Deben ser revisados y aprobados por arquitectos senior antes de finalización.

Producciones esperadas :

- Mínimo 3 ADRs documentados con estructura completa (contexto, alternativas, decisión, consecuencias)
- Diagramas de arquitectura que visualicen decisiones clave
- Documento de justificación que explique trade-offs evaluados
- Runbook operativo para al menos un procedimiento crítico

Competencias evaluadas : C17, C20

Coordinación de Proyecto de Adopción Cloud con Múltiples Stakeholders

Contexto : Un profesional debe coordinar un proyecto de adopción cloud que involucra equipos técnicos, de negocio y operaciones. Debe gestionar cronograma, recursos, riesgos y comunicar estado regularmente a stakeholders con diferentes niveles de conocimiento técnico. El proyecto tiene duración de 6 meses con múltiples fases de migración.

Restricciones : Debe mantener cronograma actualizado en herramienta de gestión de proyectos. Debe realizar reportes de estado semanales a stakeholders técnicos y mensuales a ejecutivos. Debe identificar y escalar riesgos inmediatamente. Debe documentar todas las desviaciones de cronograma y presupuesto.

Producciones esperadas :

- Plan de proyecto detallado con WBS, cronograma y asignación de recursos
- Reportes de estado semanales y mensuales con métricas de progreso
- Registro de riesgos identificados con planes de mitigación
- Comunicaciones a stakeholders adaptadas a audiencia (técnica vs. ejecutiva)
- Documento de lecciones aprendidas post-proyecto

Competencias evaluadas : C18, C19

Comunicación de Decisiones Técnicas a Audiencias Mixtas

Contexto : Un arquitecto cloud debe presentar decisiones arquitectónicas a una audiencia mixta que incluye CTO, directores de negocio, arquitectos técnicos y operaciones. Debe explicar por qué se seleccionó una arquitectura de microservicios con Kubernetes, incluyendo beneficios empresariales (agilidad, escalabilidad) y consideraciones técnicas (complejidad, costes).

Restricciones : La presentación debe ser comprensible para audiencias no técnicas sin perder rigor técnico. Debe incluir diagramas visuales claros. Debe cuantificar beneficios empresariales (reducción de time-to-market, mejora de disponibilidad). Debe ser honesto sobre trade-offs y riesgos.

Producciones esperadas :

- Presentación ejecutiva con diagramas de arquitectura y beneficios empresariales
- Documento técnico detallado con especificaciones y justificación
- Matriz de comparación de alternativas evaluadas
- Plan de mitigación de riesgos identificados
- Respuestas documentadas a preguntas frecuentes

Competencias evaluadas : C17, C20

Liderazgo de Transformación Cultural hacia Cloud

Contexto : Una organización está adoptando cloud computing y requiere transformación cultural significativa. Los equipos están acostumbrados a infraestructura on-premises y resisten cambios. Un profesional debe liderar iniciativas de capacitación, promover nuevas prácticas y ejemplificar comportamientos deseados para facilitar adopción.

Restricciones : Debe diseñar programa de capacitación adaptado a diferentes roles (arquitectos, desarrolladores, operaciones). Debe crear documentación clara y accesible. Debe facilitar sesiones de aprendizaje y mentoría. Debe medir adopción de nuevas prácticas mediante encuestas y métricas.

Producciones esperadas :

- Plan de transformación cultural con objetivos y métricas
- Programa de capacitación estructurado por roles
- Materiales de aprendizaje (guías, videos, tutoriales)
- Sesiones de mentoría documentadas
- Encuestas de adopción y feedback de equipos
- Documento de mejora continua basado en feedback

Competencias evaluadas : C19, C20

Alineación de Soluciones Cloud con Objetivos Empresariales

Contexto : Un equipo de arquitectura debe diseñar una solución cloud que alinee con objetivos empresariales específicos: reducir costes operativos en 30%, mejorar time-to-market de nuevas funcionalidades en 50% y aumentar disponibilidad de servicios a 99.99%. Debe traducir estos objetivos a especificaciones técnicas y validar que la solución propuesta los cumple.

Restricciones : Debe documentar claramente cómo cada decisión técnica contribuye a objetivos empresariales. Debe cuantificar beneficios esperados. Debe definir KPIs medibles para validar éxito post-implementación. Debe ser honesto sobre limitaciones técnicas.

Producciones esperadas :

- Documento de alineación que mapea objetivos empresariales a especificaciones técnicas
- Análisis de ROI con proyecciones de beneficios
- Definición de KPIs técnicos y empresariales
- Plan de validación post-implementación
- Documento de riesgos que podrían impedir cumplimiento de objetivos
- Propuesta de solución con justificación de decisiones

Competencias evaluadas : C17, C18, C20

Pruebas esperadas

■ Pruebas documentales

- ADRs (Architecture Decision Records) documentados con contexto, alternativas y consecuencias
- Diagramas de arquitectura cloud (C4, UML) con anotaciones de decisiones
- Runbooks operativos con procedimientos paso a paso
- Planes de proyecto con cronograma, recursos y riesgos
- Reportes de estado de proyecto con métricas de progreso
- Documentación de capacitación y programas de transformación
- Matrices de evaluación de alternativas arquitectónicas
- Análisis de alineación de soluciones con objetivos empresariales
- Documentación de lecciones aprendidas
- Especificaciones técnicas traducidas de requisitos empresariales

■ Pruebas de acción (en campo)

- Facilitación de sesiones de documentación de decisiones arquitectónicas
- Coordinación de reuniones de proyecto con múltiples stakeholders
- Presentación de decisiones técnicas a audiencias mixtas
- Liderazgo de sesiones de capacitación y mentoría
- Gestión de cronograma y recursos de proyecto
- Escalado de riesgos y problemas identificados
- Implementación de procesos de revisión y aprobación de documentación
- Facilitación de sesiones de transformación cultural
- Validación de alineación de soluciones con objetivos empresariales
- Ejecución de simulacros de procedimientos operativos

■ Pruebas reflexivas

- Análisis de efectividad de documentación en transferencia de conocimiento
- Reflexión sobre claridad de comunicación técnica a diferentes audiencias
- Evaluación de adopción de nuevas prácticas por equipos
- Análisis de desviaciones de proyecto y causas raíz

- Reflexión sobre alineación real vs. esperada con objetivos empresariales
- Evaluación de resistencia al cambio y estrategias de mitigación
- Análisis de completitud y actualización de documentación
- Reflexión sobre efectividad de liderazgo en transformación
- Evaluación de satisfacción de stakeholders con comunicación
- Análisis de mejoras necesarias en procesos de gestión de proyectos

Criterios de éxito (7 familias)

Familia	Definición	Ponderación
Conformité	La documentación técnica cumple con estándares de formato y estructura establecidos (ADRs, diagramas, runbooks)	Porcentaje de documentos que cumplen con checklist de conformidad (contexto, alternativas, decisión, consecuencias en ADRs; pasos claros en runbooks)
Qualité	La documentación es clara, precisa y completa, facilitando comprensión y transferencia de conocimiento	Evaluación de claridad por múltiples lectores (arquitectos, desarrolladores, operaciones); porcentaje de preguntas de aclaración después de lectura
Comunicación	Las decisiones técnicas se comunican de forma comprensible para audiencias técnicas y no técnicas, con justificación clara de trade-offs	Feedback de stakeholders sobre comprensión de decisiones; porcentaje de preguntas respondidas en presentaciones; evaluación de claridad de diagramas
Cohérence	Las decisiones arquitectónicas son coherentes entre sí y alineadas con objetivos empresariales y estrategia cloud	Validación de alineación entre decisiones técnicas y objetivos empresariales; identificación de inconsistencias en documentación
Traçabilité	Todas las decisiones, cambios de proyecto y comunicaciones están documentados y versionados para auditoría y trazabilidad	Completitud del registro de decisiones; frecuencia de actualización de documentación; trazabilidad de cambios en control de versiones
Pertinence	La documentación y comunicación son relevantes para audiencia específica y contexto de proyecto	Evaluación de relevancia por stakeholders; porcentaje de información utilizada en toma de decisiones; feedback sobre utilidad de documentación
Posture	El profesional demuestra rigor en documentación, responsabilidad en coordinación de proyectos, claridad en comunicación y liderazgo en transformación	Evaluación de rigor en documentación; cumplimiento de compromisos de proyecto; feedback de equipos sobre liderazgo; adopción de nuevas prácticas

Umbral de validación : Promedio ≥ 10/20

ANEXO VI Glosario y terminología

Este glosario presenta la terminología del referencial. Los términos siguientes deben utilizarse sistemáticamente en la enseñanza y la evaluación.

1. Términos profesionales obligatorios

- ADR (Architecture Decision Record)
- Arquitectura cloud escalable
- BCP (Business Continuity Plan)
- Cloud híbrida
- DAST (Dynamic Application Security Testing)
- DevSecOps
- DRP (Disaster Recovery Plan)
- Gestión de identidades y accesos (IAM)
- Hardening de servidores
- Infrastructure as Code (IaC)
- Instancias reservadas
- Integración de sistemas
- Migración de aplicaciones
- Migración de datos
- Modelo de responsabilidad compartida
- Monitoreo de rendimiento
- Orquestación de contenedores
- Patrones arquitectónicos
- Principio de mínimo privilegio
- Provisión de servicios cloud
- Rightsizing
- RPO (Recovery Point Objective)
- RTO (Recovery Time Objective)
- Runbook operativo
- SAST (Static Application Security Testing)
- Seguridad en cloud
- SLI (Service Level Indicator)
- SLO (Service Level Objective)
- Spot instances
- Transformación cloud

2. Sinónimos normalizados (forma canónica en negrita)

- Acceso mínimo → **Principio de mínimo privilegio**
- Adopción de cloud → **Transformación cloud**
- Ajuste de tamaño → **Rightsizing**
- Análisis dinámico de seguridad → **DAST (Dynamic Application Security Testing)**
- Análisis estático de seguridad → **SAST (Static Application Security Testing)**
- Configuración de seguridad → **Seguridad en cloud**
- Código IaC → **Infrastructure as Code (IaC)**
- Endurecimiento de servidores → **Hardening de servidores**
- Entorno híbrido → **Cloud híbrida**

- Gestión de accesos → **Gestión de identidades y accesos (IAM)**
- Herramientas de IaC → **Infrastructure as Code (IaC)**
- Indicador de nivel de servicio → **SLI (Service Level Indicator)**
- Instancias bajo demanda variable → **Spot instances**
- Instancias de reserva → **Instancias reservadas**
- Integración de soluciones → **Integración de sistemas**
- Monitoreo de servicios → **Monitoreo de rendimiento**
- Objetivo de nivel de servicio → **SLO (Service Level Objective)**
- Orquestación de aplicaciones → **Orquestación de contenedores**
- Plan de continuidad → **BCP (Business Continuity Plan)**
- Plan de recuperación → **DRP (Disaster Recovery Plan)**
- Procedimientos operativos → **Runbook operativo**
- Provisión de infraestructura → **Provisión de servicios cloud**
- Punto de recuperación → **RPO (Recovery Point Objective)**
- Registro de decisiones → **ADR (Architecture Decision Record)**
- Responsabilidad compartida → **Modelo de responsabilidad compartida**
- Seguridad en desarrollo → **DevSecOps**
- Tiempo de recuperación → **RTO (Recovery Time Objective)**
- Traslado de aplicaciones → **Migración de aplicaciones**
- Traslado de datos → **Migración de datos**

3. Glosario de términos

Término	Definición
ADR (Architecture Decision Record)	Documento que registra decisiones arquitectónicas importantes, incluyendo contexto, alternativas evaluadas y consecuencias.
Arquitectura cloud escalable	Diseño de sistemas cloud capaz de aumentar o disminuir recursos de forma automática y eficiente en respuesta a cambios en la demanda, manteniendo rendimiento y disponibilidad.
BCP (Business Continuity Plan)	Plan documentado que define estrategias y procedimientos para mantener operaciones críticas durante interrupciones o desastres.
Cloud híbrida	Arquitectura que integra recursos de cloud pública y cloud privada, permitiendo flexibilidad operativa y cumplimiento normativo.
DAST (Dynamic Application Security Testing)	Análisis dinámico de aplicaciones en ejecución para identificar vulnerabilidades de seguridad mediante pruebas de penetración automatizadas.
DevSecOps	Integración de prácticas de seguridad en el ciclo de vida de desarrollo de software, incluyendo análisis de vulnerabilidades y controles en pipelines.
DRP (Disaster Recovery Plan)	Plan específico que detalla procedimientos para restaurar sistemas y datos después de un evento catastrófico.
Gestión de identidades y accesos (IAM)	Sistema de control que gestiona quién puede acceder a qué recursos en cloud, aplicando autenticación, autorización y auditoría.

Término	Definición
Hardening de servidores	Proceso de configurar y asegurar servidores cloud eliminando vulnerabilidades, aplicando parches de seguridad y deshabilitando servicios innecesarios.
Infrastructure as Code (IaC)	Práctica de definir y gestionar infraestructura cloud mediante código versionado y automatizado, utilizando herramientas como Terraform, CloudFormation o Pulumi.
Instancias reservadas	Compromiso de compra a largo plazo de capacidad cloud que ofrece descuentos significativos comparado con precios bajo demanda.
Integración de sistemas	Conexión y comunicación entre soluciones cloud y sistemas heredados mediante APIs, colas de mensajes o buses de eventos.
Migración de aplicaciones	Proceso de trasladar aplicaciones desde entornos on-premises a cloud, utilizando estrategias como rehost, replatform o refactor.
Migración de datos	Transferencia de datos desde sistemas heredados a plataformas cloud garantizando integridad, seguridad y validación.
Modelo de responsabilidad compartida	Marco que define qué componentes de seguridad son responsabilidad del proveedor cloud y cuáles del cliente en cada modelo de servicio.
Monitoreo de rendimiento	Supervisión continua de métricas, trazas distribuidas y logs de servicios cloud para evaluar disponibilidad, latencia, throughput y detectar anomalías.
Orquestación de contenedores	Automatización del despliegue, escalado y gestión del ciclo de vida de contenedores en plataformas como Kubernetes.
Patrones arquitectónicos	Soluciones reutilizables para problemas comunes de diseño en arquitecturas cloud, incluyendo microservicios, serverless y contenedores.
Principio de mínimo privilegio	Práctica de seguridad que otorga a usuarios y aplicaciones solo los permisos mínimos necesarios para realizar sus funciones.
Provisión de servicios cloud	Proceso de crear, configurar y desplegar recursos cloud públicos (AWS, Azure, GCP) de forma automatizada y reproducible.
Rightsizing	Proceso de ajustar el tamaño y tipo de instancias cloud para optimizar costes sin comprometer rendimiento o disponibilidad.
RPO (Recovery Point Objective)	Cantidad máxima de datos que se puede perder, medida en tiempo, en caso de interrupción o desastre.
RTO (Recovery Time Objective)	Tiempo máximo aceptable para restaurar un servicio o sistema después de una interrupción o desastre.
Runbook operativo	Documento con procedimientos paso a paso para ejecutar tareas operativas comunes como despliegue, escalado o recuperación ante incidentes.

Término	Definición
SAST (Static Application Security Testing)	Análisis estático de código fuente para identificar vulnerabilidades de seguridad sin ejecutar la aplicación.
Seguridad en cloud	Conjunto de controles técnicos y procedimientos para proteger datos, aplicaciones e infraestructura en entornos cloud contra amenazas y accesos no autorizados.
SLI (Service Level Indicator)	Métrica cuantificable que mide el rendimiento real de un servicio cloud, como latencia, disponibilidad o tasa de error.
SLO (Service Level Objective)	Objetivo de rendimiento establecido para un servicio cloud, expresado como un rango aceptable de SLIs que debe cumplirse.
Spot instances	Instancias cloud ofrecidas a precios reducidos con disponibilidad variable, ideales para cargas de trabajo tolerantes a interrupciones.
Transformación cloud	Proceso organizativo de adoptar tecnologías y prácticas cloud, incluyendo cambio cultural, capacitación y alineación con objetivos empresariales.