CCSP® – Certified Cloud Security Professional (e-Learning)

ISC2

- **Nível:**
- **Duração:** 35h

Sobre o curso

Prepara-te para obter a certificação CCSP – Certified Cloud Security Professional, reconhecida globalmente. Desenvolve a tua carreira e protege de forma eficaz ativos críticos em cloud.

A certificação CCSP demonstra que possuis as competências técnicas avançadas e os conhecimentos necessários para desenhar, gerir e proteger dados, aplicações e infraestrutura em cloud, com base em boas práticas, políticas e procedimentos estabelecidos pelos nossos membros certificados e especialistas em cibersegurança em todo o mundo.

Comprova as tuas competências, impulsiona a tua carreira e beneficia do apoio de uma comunidade de líderes em cibersegurança, pronta para te acompanhar ao longo do teu percurso profissional.

Destinatários

A certificação CCSP é ideal para líderes de IT, cibersegurança, segurança da informação e segurança de software responsáveis por aplicar boas práticas à arquitetura, design, operações e orquestração de serviços em cloud, incluindo profissionais nas seguintes funções:

- Cloud Architect
- Cloud Engineer
- Cloud Consultant
- Cloud Administrator
- Cloud Security Analyst
- Cloud Specialist
- Auditor de Serviços de Cloud Computing
- Professional Cloud Developer

Objetivos

- Descrever a arquitetura de referência de cloud.

- Indicar os princípios de design de cloud computing segura.
- Implementar a segurança de dados em cloud.
- Aplicar a segurança da plataforma e infraestrutura cloud.
- Aplicar a segurança de aplicações em cloud.
- Construir operações de segurança em cloud.
- Preparar o cumprimento de requisitos legais, de risco e de conformidade.

Pré-requisitos

Para obter esta certificação, é necessário passar no exame e possuir pelo menos cinco anos de experiência profissional cumulativa em tecnologias de informação, dos quais três anos devem ser em segurança da informação e um ano em um ou mais dos seis domínios do ISC2 CCSP Exam Outline.

Metodologia

A Formação Oficial ISC2 Online Self-Paced CCSP é uma forma inovadora de preparação para a certificação que utiliza inteligência artificial para personalizar o teu percurso de aprendizagem. Identifica as áreas que exigem foco adicional e orienta-te na preparação para o exame de forma verdadeiramente personalizada.

Estuda de forma mais inteligente com estas principais vantagens:

- **Instrução personalizada** – O conteúdo, o ritmo e a dificuldade adaptam-se ao teu nível de conhecimento, velocidade de aprendizagem e nível de confiança.
- **Maior envolvimento** – Feedback imediato e conteúdo dinâmico permitem-te aprender a um nível adequado.
- **Poupança de tempo** – O tempo de formação é otimizado ao focar-se nas áreas que exigem maior revisão.
- **Melhores resultados de aprendizagem** – A plataforma identifica as áreas que exigem revisão adicional e disponibiliza suporte direcionado para maximizar a tua compreensão do conteúdo.

A formação Certified Cloud Security Professional (CCSP) tira partido do poder da inteligência artificial, orientando os formandos numa experiência de aprendizagem ao seu ritmo, adaptada às suas necessidades. Abrange as competências técnicas avançadas e os conhecimentos necessários para desenhar, gerir e proteger dados, aplicações e infraestrutura em cloud.

Programa

- Conceitos, Arquitetura e Design de Cloud
- Segurança de Dados em Cloud
- Segurança da Plataforma e Infraestrutura Cloud
- Segurança de Aplicações em Cloud
- Operações de Segurança em Cloud

- Legal, Risco e Conformidade

Domínio 1: Conceitos, Arquitetura e Design de Cloud

Compreender os conceitos de cloud computing

- Definições de cloud computing
- Papéis e responsabilidades em cloud computing (por exemplo, cloud service customer, cloud service provider, cloud service partner, cloud service broker, regulador)
- Principais características de cloud computing (por exemplo, on-demand self-service, broad network access, multi-tenancy, rapid elasticity e escalabilidade, resource pooling, measured service)
- Tecnologias base (por exemplo, virtualização, storage, networking, bases de dados, orquestração)

Descrever a arquitetura de referência de cloud

- Atividades de cloud computing
- Capacidades dos serviços cloud (por exemplo, tipos de application capability, tipos de platform capability, tipos de infrastructure capability)
- Categorias de serviços cloud (por exemplo, Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Modelos de deployment cloud (por exemplo, public, private, hybrid, community, multi-cloud)
- Considerações transversais de cloud (por exemplo, interoperabilidade, portabilidade, reversibilidade, disponibilidade, segurança, privacidade, resiliência, desempenho, governação, manutenção e versionamento, níveis de serviço e service-level agreements (SLA), auditabilidade, regulamentação, outsourcing)
- Impacto de tecnologias relacionadas (por exemplo, data science, machine learning, artificial intelligence (AI), blockchain, Internet of Things (IoT), containers, quantum computing, edge computing, confidential computing, DevSecOps)

Compreender conceitos de segurança relevantes para cloud computing

- Criptografia e gestão de chaves
- Identidade e controlo de acessos (por exemplo, acesso de utilizador, acesso privilegiado, acesso a serviços)
- Sanitização de dados e suportes (por exemplo, overwriting, cryptographic erase)
- Segurança de rede (por exemplo, network security groups, inspeção de tráfego, geofencing, zero trust network)
- Segurança da virtualização (por exemplo, segurança do hypervisor, segurança de containers, ephemeral computing, tecnologia serverless)
- Ameaças comuns
- Higiene de segurança (por exemplo, patching, definição de baselines)

Compreender os princípios de design de cloud computing segura

- Ciclo de vida seguro dos dados em cloud
- Plano de business continuity (BC) e disaster recovery (DR) baseado em cloud
- Business impact analysis (BIA) (por exemplo, análise custo-benefício, return on investment (ROI))

- Requisitos funcionais de segurança (por exemplo, portabilidade, interoperabilidade, vendor lock-in)
- Considerações e responsabilidades de segurança para diferentes categorias de cloud (por exemplo, Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Cloud design patterns (por exemplo, princípios de segurança SANS, Well-Architected Framework, Cloud Security Alliance (CSA) Enterprise Architecture)
- Segurança em DevOps

Avaliar fornecedores de serviços cloud

- Verificação face a critérios (por exemplo, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27017, Payment Card Industry Data Security Standard (PCI DSS))
- Certificações de produtos de sistema/subsistema (por exemplo, Common Criteria (CC), Federal Information Processing Standard (FIPS) 140-2)

Domínio 2: Segurança de Dados em Cloud

Descrever conceitos de dados em cloud

- Fases do ciclo de vida dos dados em cloud
- Dispersão de dados
- Fluxos de dados

Desenhar e implementar arquiteturas de armazenamento de dados em cloud

- Tipos de armazenamento (por exemplo, long-term, ephemeral, raw storage)
- Ameaças aos tipos de armazenamento

Desenhar e aplicar tecnologias e estratégias de segurança de dados

- Encriptação e gestão de chaves
- Hashing
- Ofuscação de dados (por exemplo, masking, anonymization)
- Tokenização
- Data loss prevention (DLP)
- Gestão de chaves, segredos e certificados

Implementar data discovery

- Dados estruturados
- Dados não estruturados
- Dados semiestruturados
- Localização dos dados

Planear e implementar a classificação de dados

- Políticas de classificação de dados
- Data mapping
- Data labeling

Desenhar e implementar Information Rights Management (IRM)

- Objetivos (por exemplo, direitos sobre os dados, provisioning, modelos de acesso)
- Ferramentas adequadas (por exemplo, emissão e revogação de certificados)

Planear e implementar políticas de retenção, eliminação e arquivo de dados

- Políticas de retenção de dados
- Procedimentos e mecanismos de eliminação de dados
- Procedimentos e mecanismos de arquivo de dados
- Legal hold

Desenhar e implementar auditabilidade, rastreabilidade e responsabilização de eventos de dados

- Definição de fontes de eventos e requisitos de atributos de eventos (por exemplo, identidade, endereço Internet Protocol (IP), geolocalização)
- Registo, armazenamento e análise de eventos de dados
- Chain of custody e non-repudiation

Domínio 3: Segurança da Plataforma e Infraestrutura Cloud

Compreender os componentes da infraestrutura e plataforma cloud

- Ambiente físico
- Rede e comunicações
- Compute
- Virtualização
- Storage
- Plano de gestão

Desenhar um data center seguro

- Design lógico (por exemplo, segmentação de tenants, controlo de acessos)
- Design físico (por exemplo, localização, buy or build)
- Design ambiental (por exemplo, Heating, Ventilation, and Air Conditioning (HVAC), conectividade multi-vendor)
- Design resiliente

Analisar riscos associados à infraestrutura e plataformas cloud

- Avaliação de risco (por exemplo, identificação, análise)
- Vulnerabilidades, ameaças e ataques em cloud
- Estratégias de mitigação de risco

Planear e implementar controlos de segurança

- Proteção física e ambiental (por exemplo, on-premises)
- Proteção de sistemas, storage e comunicações
- Identificação, autenticação e autorização em ambientes cloud

- Mecanismos de auditoria (por exemplo, recolha de logs, correlação, packet capture)

Planear business continuity (BC) e disaster recovery (DR)

- Estratégia de business continuity (BC) / disaster recovery (DR)
- Requisitos de negócio (por exemplo, Recovery Time Objective (RTO), Recovery Point Objective (RPO), nível de serviço de recuperação)
- Criação, implementação e teste do plano

Domínio 4: Segurança de Aplicações em Cloud

Promover formação e sensibilização para a segurança de aplicações

- Fundamentos de desenvolvimento em cloud
- Erros comuns
- Vulnerabilidades comuns em cloud (por exemplo, Open Web Application Security Project (OWASP) Top-10, SANS Top-25)

Descrever o processo Secure Software Development Life Cycle (SDLC)

- Requisitos de negócio
- Fases e metodologias (por exemplo, design, code, test, maintain, waterfall vs. agile)

Aplicar o Secure Software Development Life Cycle (SDLC)

- Riscos específicos de cloud
- Threat modeling (por exemplo, STRIDE, DREAD, ATASM, PASTA)
- Evitar vulnerabilidades comuns durante o desenvolvimento
- Secure coding (por exemplo, Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS), Software Assurance Forum for Excellence in Code (SAFECode))
- Gestão de configuração e versionamento de software

Aplicar software assurance e validação em cloud

- Testes funcionais e não funcionais
- Metodologias de testes de segurança (por exemplo, blackbox, whitebox, static, dynamic, Software Composition Analysis (SCA), interactive application security testing (IAST))
- Quality assurance (QA)
- Testes de abuse case

Utilizar software seguro validado

- Proteção de application programming interfaces (API)
- Supply-chain management (por exemplo, avaliação de fornecedores)
- Gestão de software de terceiros (por exemplo, licenciamento)
- Software open-source validado

Compreender as especificidades da arquitetura de aplicações em cloud

- Componentes adicionais de segurança (por exemplo, web application firewall (WAF), Database Activity Monitoring (DAM), XML firewalls, API gateway)
- Criptografia
- Sandboxing
- Virtualização e orquestração de aplicações (por exemplo, microservices, containers)

Desenhar soluções adequadas de Identity and Access Management (IAM)

- Identidade federada
- Identity providers (IdP)
- Single sign-on (SSO)
- Multi-factor authentication (MFA)
- Cloud access security broker (CASB)
- Gestão de segredos

Domínio 5: Operações de Segurança em Cloud

Construir e implementar infraestrutura física e lógica para ambiente cloud

- Requisitos específicos de configuração de segurança de hardware (por exemplo, hardware security module (HSM) e Trusted Platform Module (TPM))
- Instalação e configuração de ferramentas de gestão
- Requisitos específicos de configuração de segurança de hardware virtual (por exemplo, rede, storage, memória, central processing unit (CPU), Hypervisor tipo 1 e 2)
- Instalação de toolsets de virtualização do sistema operativo guest (OS)

Operar e manter infraestrutura física e lógica para ambiente cloud

- Controlos de acesso local e remoto (por exemplo, Remote Desktop Protocol (RDP), acesso seguro a terminal, Secure Shell (SSH), mecanismos de acesso baseados em consola, jumpboxes, virtual client)
- Configuração segura de rede (por exemplo, virtual local area networks (VLAN), Transport Layer Security (TLS), Dynamic Host Configuration Protocol (DHCP), Domain Name System Security Extensions (DNSSEC), virtual private network (VPN))
- Controlos de segurança de rede (por exemplo, firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, avaliações de vulnerabilidades, network security groups, bastion host)
- Hardening do sistema operativo (OS) através da aplicação de baselines, monitorização e remediação (por exemplo, Windows, Linux, VMware)
- Patch management
- Estratégia Infrastructure as Code (IaC)
- Disponibilidade de hosts em cluster (por exemplo, distributed resource scheduling, dynamic optimization, storage clusters, maintenance mode, high availability (HA))
- Disponibilidade do sistema operativo guest (OS)
- Monitorização de desempenho e capacidade (por exemplo, rede, compute, storage, tempo de resposta)
- Monitorização de hardware (por exemplo, disco, CPU, velocidade da ventoinha, temperatura)
- Configuração de funções de backup e restore do sistema operativo host e guest (OS)
- Plano de gestão (por exemplo, agendamento, orquestração, manutenção)

Implementar controlos e normas operacionais (por exemplo, ITIL, ISO/IEC 20000-1)

- Gestão de mudanças
- Gestão da continuidade
- Gestão da segurança da informação
- Gestão da melhoria contínua de serviços
- Gestão de incidentes
- Gestão de problemas
- Gestão de releases
- Gestão de deployment
- Gestão de configuração
- Gestão de níveis de serviço
- Gestão da disponibilidade
- Gestão da capacidade

Suportar digital forensics

- Metodologias de recolha de dados forenses
- Gestão de evidências
- Recolher, adquirir e preservar evidência digital

Gerir a comunicação com as partes relevantes

- Fornecedores
- Clientes
- Parceiros
- Reguladores
- Outros stakeholders

Gerir operações de segurança

- Security operations center (SOC)
- Monitorização inteligente de controlos de segurança (por exemplo, firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), honeypots, network security groups, artificial intelligence (AI))
- Captura e análise de logs (por exemplo, security information and event management (SIEM), log management)
- Gestão de incidentes
- Avaliações de vulnerabilidades

Domínio 6: Legal, Risco e Conformidade

Articular requisitos legais e riscos específicos no ambiente cloud

- Legislação internacional conflituante
- Avaliação de riscos legais específicos de cloud computing
- Enquadramento legal e orientações
- eDiscovery (por exemplo, ISO/IEC 27050, CSA Guidance)
- Requisitos forenses

Compreender questões de privacidade

- Diferença entre dados privados contratuais e regulamentados (por exemplo, protected health information (PHI), personally identifiable information (PII))
- Legislação específica por país relacionada com dados privados (por exemplo, PHI, PII)
- Diferenças jurisdicionais em privacidade de dados
- Requisitos padrão de privacidade (por exemplo, ISO/IEC 27018, Generally Accepted Privacy Principles (GAPP), General Data Protection Regulation (GDPR))
- Privacy Impact Assessments (PIA)

Compreender o processo de auditoria, metodologias e adaptações necessárias para ambiente cloud

- Controlos de auditoria internos e externos
- Impacto dos requisitos de auditoria
- Identificar desafios de assurance em virtualização e cloud
- Tipos de relatórios de auditoria (por exemplo, SSAE, SOC, ISAE)
- Restrições das declarações de âmbito de auditoria (por exemplo, SSAE, ISAE)
- Gap analysis (por exemplo, análise de controlos, baselines)
- Planeamento de auditoria
- Sistema interno de gestão de segurança da informação
- Sistema interno de controlos de segurança da informação
- Políticas (por exemplo, organizacionais, funcionais, cloud computing)
- Identificação e envolvimento de stakeholders relevantes
- Requisitos de conformidade especializados para indústrias altamente reguladas (por exemplo, NERC / CIP, HIPAA, HITECH Act, PCI)
- Impacto do modelo de IT distribuído (por exemplo, múltiplas localizações geográficas e diferentes jurisdições legais)

Compreender as implicações de cloud na gestão de risco empresarial

- Avaliar programas de gestão de risco dos fornecedores (por exemplo, controlos, metodologias, políticas, perfil de risco, apetite ao risco)
- Diferença entre data owner/controller e data custodian/processor
- Requisitos de transparência regulamentar (por exemplo, notificação de violação, SOX, GDPR)
- Tratamento do risco (isto é, evitar, mitigar, transferir, partilhar, aceitar)
- Diferentes frameworks de risco
- Métricas para gestão de risco
- Avaliação do ambiente de risco (por exemplo, serviço, fornecedor, infraestrutura, negócio)

Compreender outsourcing e design contratual em cloud

- Requisitos de negócio (por exemplo, service-level agreement (SLA), master service agreement (MSA), statement of work (SOW))
- Gestão de fornecedores (por exemplo, avaliações de fornecedores, riscos de vendor lock-in, viabilidade do fornecedor, escrow)
- Gestão contratual (por exemplo, direito de auditoria, métricas, definições, rescisão, litígios, assurance, conformidade, acesso a cloud/dados, seguro de risco cibernético)

- Supply-chain management (por exemplo, ISO/IEC 27036)