CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

Descrição do Exame de **Certificação**

Data efetiva: 1º de maio de 2021

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

Sobre o CISSP

O Profissional certificado de segurança de sistemas de informação (CISSP) é a certificação mais reconhecida mundialmente no mercado de segurança da informação. O CISSP valida o profundo conhecimento técnico e gerencial de um profissional de segurança da informação assim como a sua experiência para conceber, projetar e gerenciar a postura geral da segurança de uma organização eficazmente.

O amplo espectro de tópicos incluídos no CISSP Common Body of Knowledge (CBK®) garante sua relevância em todas as disciplinas no campo da segurança da informação. Os candidatos bem-sucedidos são competentes nos seguintes oito domínios:

- Segurança e Gestão de Riscos
- Segurança de Ativos
- Arquitetura e Engenharia de Segurança
- Segurança de Comunicação e Rede
- Gestão De Identidades E Acesso (IAM)
- Avaliação e Teste de Segurança
- Operações de Segurança
- Segurança no Desenvolvimento de Software

Requisitos de Experiência

Os candidatos devem ter um mínimo de cinco anos de experiência profissional remunerada cumulativa em dois ou mais dos oito domínios do CISSP CBK. Conquistando um diploma universitário de quatro anos ou equivalente regional ou uma credencial adicional da lista aprovada do (ISC)² satisfará um ano da experiência exigida. O crédito educacional só satisfará um ano de experiência.

Um candidato sem a experiência necessária para se tornar um CISSP pode tornar-se um Associado do (ISC)² ao ser aprovado no exame de CISSP. O associado do (ISC)² terá então seis anos para adquirir os cinco anos de experiência exigidos. Poderá aprender mais sobre os requisitos de experiência do CISSP e como contabilizar o trabalho de meio período e estágios em www.isc2.org/Certifications/CISSP/experience-requirements.

Acreditação

O CISSP foi a primeira credencial no campo da segurança da informação a atender aos rigorosos requisitos do padrão ANSI/ISO/IEC 17024.

Análise das Tarefas de Trabalho (JTA)

(ISC)² tem uma obrigação para com seus membros de manter a relevância do CISSP. Conduzida em intervalos regulares, a Análise das Tarefas de Trabalho (do inglês JTA - Job Task Analysis) é um processo metódico e crítico de determinar as tarefas que são executadas pelos profissionais de segurança que estão engajados na profissão definida pelo CISSP. Os resultados da JTA são usados para atualizar o exame. Este processo garante que os candidatos sejam testados nas áreas de temáticas relevantes para as funções e responsabilidades dos profissionais de segurança da informação.

Informações do Exame de CAT do CISSP

O exame do CISSP usa Testes Adaptativos Computadorizados (do inglês, Computerized Adaptive Testing – CAT) para todos os exames em Inglês. Exames CISSP em todos os outros idiomas são aplicados como exames lineares de formato fixo. Aprenda mais sobre CISSP CAT em www.isc2.org/certificatons/CISSP-CAT.

Duração do exame	3 horas
Número dos itens	100 - 150
Formato dos itens	Escolha múltipla e itens inovadores avançados
Nota de aprovação	700 em 1000 pontos
Disponibilidade de idioma para exames	Inglês
Centros de testes	Centros de Testes Autorizados (ISC)² da Pearson VUE PPC e PVTC Selecionados

Pesos do Exame CISSP CAT

Domínios	Percentagem Média
1. Segurança e Gestão de Riscos	15%
2. Segurança de Ativos	10%
3. Arquitetura e Engenharia de Segurança	13%
4. Segurança de Comunicação e Rede	13%
5. Gestão De Identidades E Acesso (IAM)	13%
6. Avaliação e Teste de Segurança	12%
7. Operações de Segurança	13%
8. Segurança no Desenvolvimento de Software	11%
Total:	**100%**

Informações sobre o Exame Linear CISSP

Duração do exame	6 horas
Número dos itens	250
Formato dos itens	Escolha múltipla e itens inovadores avançados
Nota de aprovação	700 em 1000 pontos
Disponibilidade de idioma para exames	Francês, alemão, português do Brasil, espanhol moderno, japonês, chinês simplificado, coreano
Centros de testes	Centros de Testes Autorizados (ISC)² da Pearson VUE PPC e PVTC Selecionados

Quotas de exame linear CISSP

Domínios	Peso
1. Segurança e Gestão de Riscos	15%
2. Segurança de Ativos	10%
3. Arquitetura e Engenharia de Segurança	13%
4. Segurança de Comunicação e Rede	13%
5. Gestão De Identidades E Acesso (IAM)	13%
6. Avaliação e Teste de Segurança	12%
7. Operações de Segurança	13%
8. Segurança no Desenvolvimento de Software	11%
Total:	**100%**

Domínio 1: Segurança e Gestão de Riscos

1.1 Entender, cumprir e promover a ética profissional

- Código de Ética Profissional do (ISC)²
- Código de ética organizacional

1.2 Entender e aplicar conceitos de segurança

- Confidencialidade, integridade e disponibilidade, autenticidade e não repúdio

1.3 Avaliar e aplicar princípios de governança de segurança

- Alinhamento da função de segurança com a estratégia, metas, missão e objetivos de negócios
- Processos organizacionais (por exemplo, aquisições, alienações, comitês de governança)
- Papéis e responsabilidades organizacionais
- Estruturas de controle de segurança
- Cuidado / diligência devida

1.4 Determinar requisitos de conformidade e outros

- Requisitos contratuais, legais, padrões da indústria e regulatórios
- Requisitos de privacidade

1.5 Entender questões legais e regulatórias que se referem a segurança da informação em um contexto holístico

- Crimes cibernéticos e violação de dados
- Requisitos de licenciamento e propriedade intelectual
- Controles de importação/exportação
- Fluxo de dados transfronteiriço
- Privacidade

1.6 Entender os requisitos para tipos de investigação (ou seja, administrativo, penal, civil, regulatórios, padrões do setor)

1.7 Desenvolver, documentar e implementar políticas, padrões, procedimentos e diretrizes de segurança

1.8 Identificar, analisar e priorizar requisitos de Continuidade de Negócios (BC)

- Análise de Impacto de Negócios (AIN)
- Desenvolver e documentar o escopo e plano

1.9 Contribuir e reforçar políticas e procedimentos de segurança de pessoal

- Seleção e contratação de candidatos
- Contratos e políticas de emprego
- Processos de integração, transferências e rescisão
- Contratos e controles de fornecedores, consultores e de empreiteiros
- Requisitos de política de conformidade
- Requisitos de política de privacidade

1.10 Entender e aplicar conceitos de gerenciamento de riscos

- Identificar ameaças e vulnerabilidades
- Avaliação/análise de riscos
- Resposta a riscos
- Seleção e implementação de contramedidas
- Tipos aplicáveis de controles (p.ex., preventivo, detecção, corretivo)
- Avaliação de controles (segurança e privacidade)
- Monitoramento e medição
- Elaboração de relatório
- Melhoria contínua (p. ex., modelagem de maturidade de risco)
- Estruturas de risco

1.11 Entender e aplicar conceitos e metodologias de modelagem de ameaças

1.12 Aplicar conceitos de gestão de risco da cadeia de abastecimento (SCRM)

- Riscos Associados com hardware, software e serviços
- Avaliação e monitoramento de terceiros
- Requisitos mínimos de segurança
- Requisitos de Nível de Serviço

1.13 Estabelecer e manter um programa de conscientização, educação e treinamento de segurança

- Métodos e técnicas para conscientização e capacitação (por exemplo, engenharia social, phishing, campeões de segurança, gamificação)
- Revisões periódicas de conteúdo
- Avaliação da eficácia do programa

Domínio 2: Segurança de Ativos

2.1 Identificar e classificar informações e ativos

» Classificação de dados
» Classificação de Ativos

2.2 Estabelecer requisitos de manuseio de informações e ativos

2.3 Provisionar recursos em segurança

» Informações e propriedade de ativos
» Inventário de ativos (p. ex., tangíveis, intangíveis)
» Gerenciamento de ativos

2.4 Gerenciar o ciclo de vida de dados

» Funções de dados (ou seja, proprietários, controladores, custodiantes, processadores, usuários / sujeitos)
» Coleta de dados
» Localização de dados
» Manutenção de dados
» Retenção de dados
» Remanência de dados
» Destruição de dados

2.5 Garantir a retenção de ativos adequada (por exemplo, Fim-de-vida (EOL), fim do suporte (EOS))

2.6 Determinar controles de segurança de dados e requisitos de conformidade

» Estados dos dados (por exemplo, em uso, em trânsito, em repouso)
» Escopo e personalização
» Seleção de padrões
» Métodos de proteção de dados (p. ex., Gestão de Direitos Digitais (GDD), Prevenção de Perda de Dados (Data Loss Prevention - DLP), corretor de segurança de acesso à nuvem- CASB)

Domínio 3: Arquitetura e Engenharia de Segurança

3.1 Pesquisar, implementar e gerenciar processos de engenharia usando princípios de projeto seguro

- Modelagem de Ameaça
- Privilégio mínimo
- Defesa em profundidade
- Padrões seguros
- Falha com segurança
- Separação de Deveres (SoD)
- Manter simples
- Confiança Zero
- Confiança Zero por design
- Confie mas verifique
- Responsabilidade compartilhada

3.2 Entender os conceitos fundamentais de modelos de segurança (p. ex., Biba, Star Model, Bell-LaPadula)

3.3 Selecionar controles baseados em requisitos de segurança de sistemas

3.4 Entender as capacidades de segurança dos sistemas de informações (SI) (p.ex., proteção de memória, Módulo de Plataforma Confiável (TPM), criptografia/descriptografia)

3.5 Avaliar e mitigar as vulnerabilidades de segurança dos elementos de arquiteturas, projetos e soluções

- Sistemas baseados em cliente
- Sistemas baseados em servidor
- Sistemas de base de dados
- Sistemas criptográficos
- Sistemas de Controle Industrial (ICS)
- Sistemas baseados em nuvem (por exemplo, Software Como Serviço (SaaS), Infraestrutura Como Serviço (IaaS), Plataforma como serviço (PaaS))
- Sistemas distribuídos
- Internet das Coisas (IoT)
- Micro serviços
- Conteinerização
- Sem servidor
- Sistemas integrados
- Sistemas de Computação de Alta Performance (HPC)
- Sistemas de computação de borda
- Sistemas virtualizados

3.6 Selecionar e determinar soluções de criptografia

- Ciclo de vida criptográfico (por exemplo, chaves, seleção de algoritmo)
- Métodos criptográficos (por exemplo, curvas simétricas, assimétricas, elípticas, quânticas)
- Infraestrutura de Chaves Públicas (ICP)
- Principais práticas de gestão
- Assinaturas digitais e certificados digitais
- Não repúdio
- Integridade (por exemplo, hashing)

3.7 Compreender os métodos de ataques criptoanalíticos

- Força bruta
- Texto cifrado apenas
- Texto simples conhecido
- Análise de frequência
- Texto cifrado escolhido
- Ataques de implementação
- Canal lateral
- Injeção de falha
- Temporização
- Mediador (MITM)
- Transferir o hash
- Exploração Kerberos
- Ransomware

3.8 Aplicar princípios de segurança a projeto do site e instalações

3.9 Projetar controles de segurança do site e das instalações

- Gabinetes de fiação/instalações de distribuição intermediárias
- Salas de servidores/data centers
- Instalações de armazenamento de mídia
- Armazenamento de evidências
- Segurança restrita e área de trabalho
- Aquecimento, Ventilação e Ar-condicionado (HVAC)
- Questões ambientais
- Prevenção, detecção e supressão de incêndio
- Energia (por exemplo, redundante, backup)

Domínio 4: Segurança da Comunicação e Rede

4.1 Avaliar e implementar princípios de projeto seguro em arquiteturas de rede

- Modelos de Open System Interconnection (OSI) e Transmission Control Protocol/Protocolo de Internet (TCP/IP)
- Rede de protocolo da Internet (IP) (por exemplo, Segurança de protocolo da Internet (IPSec), Internet Protocol (IP) v4/6)
- Protocolos seguros
- Implicações de protocolos multicamadas
- Protocolos convergentes (por exemplo, Fibre Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Protocolo de Internet sobre voz(VoIP))
- Microssegmentação (por exemplo, Redes definidas por software (SDN), Rede local virtual eXtensível(VXLAN), Encapsulamento, Rede de longa distância definida por software (SD-WAN))
- Redes sem fio (por exemplo, Li-Fi, Wi-Fi, Zigbee, satélite)
- Redes de celular (por exemplo, 4G, 5G)
- Redes de distribuição de conteúdo (CDN)

4.2 Componentes de rede segura

- Operação de hardware (por exemplo, alimentação redundante, garantia, suporte)
- Meio de transmissão
- Dispositivos de Controle de Acesso à Rede (NAC)
- Segurança de endpoint

4.3 Implementar canais de comunicação segura de acordo com o projeto

- Voz
- Colaboração multimídia
- Acesso Remoto
- Comunicações de dados
- Redes virtualizadas
- Conectividade de terceiros

Domínio 5: Gestão De Identidades E Acesso (IAM)

5.1 Controlar o acesso físico e lógico aos ativos

- Informações
- Sistemas
- Dispositivos
- Instalações
- Aplicações

5.2 Gerenciar identificação e autenticação de pessoas, dispositivos e serviços

- Implementação de gerenciamento de identidade (IdM)
- Autenticação de fator único / multifator (MFA)
- Responsabilidade
- Gerenciamento da Sessão
- Registro, prova e estabelecimento de identidade
- Gestão de identidade federada (FIM)
- Sistemas de gerenciamento de credenciais
- Logon único (SSO)
- Na hora certa (JIT)

5.3 Identidade federada com um serviço de terceiros

- Presencial
- Nuvem
- Híbrido

5.4 Implementar e gerenciar mecanismos de autorização

- Controle de Acesso Baseado em Função (RBAC)
- Controle de acesso baseado em regras
- Controle de Acesso Obrigatório (MAC)
- Controle de Acesso Discricionário (DAC)
- Controle de Acesso Baseado em Atributos (ABAC)
- Controle de acesso baseado em risco

5.5 Gerenciar o ciclo de vida de aprovisionamento de identidade e acesso

- Revisão de acesso à conta (por exemplo, usuário, sistema, serviço)
- Provisionamento e desprovisionamento (por exemplo, on/off boarding e transferências)
- Definição de função (por exemplo, pessoas atribuídas a novas funções)
- Escalonamento de privilégios (por exemplo, contas de serviço gerenciado, uso de sudo, minimizando seu uso)

5.6 Implementar sistemas de autenticação

- OpenID Connect (OIDC) / Autorização Aberta (Oauth)
- Linguagem De Marcação Para Declaração De Segurança (SAML)
- Kerberos
- Serviço de Autenticação Remota de Usuário Discado (RADIUS) /Terminal Access Controller Access Control System Plus (TACACS+)

Domínio 6: Avaliação e Teste de Segurança

6.1 Projetar e validar estratégias de avaliação, teste e auditoria

- Interno
- Externo
- Terceiros

6.2 Conduzir testes de controle de segurança

- Avaliação de vulnerabilidade
- Teste de penetração
- Revisões de registros
- Transações sintéticas
- Revisão e teste de código
- Teste de caso de uso indevido
- Análise de cobertura de teste
- Teste de interface
- Simulações de ataque de violação
- Verificações de conformidade

6.3 Coletar dados de processo de segurança (p.ex. técnico e administrativo)

- Gerenciamento de contas
- Gerenciamento de revisão e aprovação
- Principais indicadores de desempenho e risco
- Dados de verificação de backup
- Treinamento e conhecimento
- Recuperação de desastres (DR) e continuidade de negócios (BC)

6.4 Analisar resultados de teste e gerar relatório

- Remediação
- Manipulação de exceção
- Divulgação ética

6.5 Conduzir ou facilitar auditorias de segurança

- Interno
- Externo
- Terceiros

Domínio 7: Operações de Segurança

7.1 Entender e cumprir as investigações

- Coleta e manuseio de evidência
- Elaboração de relatórios e documentação
- Técnicas de investigação
- Ferramentas, táticas e procedimentos forenses
- Artefatos (por exemplo, computador, rede, dispositivo móvel)

7.2 Realizar atividades de registro e monitoramento

- Detecção e prevenção de intrusão
- Informação de segurança e gestão de eventos (SIEM)
- Monitoramento contínuo
- Monitoramento de saída
- Gerenciamento de log
- Inteligência de ameaças (por exemplo, feeds de ameaças, caça a ameaças)
- Análise Comportamental de Usuários e Entidade (UEBA)

7.3 Executar o Gestão de Configuração (CM) (por exemplo, provisionamento, baselining, automação)

7.4 Aplicar conceitos fundamentais de segurança de operações

- Preciso saber / privilégio mínimo
- Separação de deveres (SoD) e responsabilidades
- Gerenciamento de contas privilegiadas
- Rotação de trabalho
- Acordo de nível de serviço (SLAs)

7.5 Aplicar proteção de recursos

- Gerenciamento de mídia
- Técnicas de proteção de mídia

7.6 Conduzir gerenciamento de incidentes

- Detecção
- Resposta
- Mitigação
- Elaboração de relatório
- Recuperação
- Remediação
- Lições aprendidas

7.7 Operar e manter medidas de detecção e prevenção

- Firewalls (por exemplo, próxima geração, aplicativo web, rede)
- Sistemas de detecção de intrusão (IDS) e Sistemas de prevenção de intrusão (IPS)
- Whitelisting/blacklisting
- Serviços de segurança fornecidos por terceiros
- Sandboxing
- Honeypots/honeynets
- Anti-malware
- Ferramentas baseadas em aprendizado de máquina e inteligência artificial (IA)

7.8 Implementar e suportar gerenciamento de patch e vulnerabilidade

7.9 Entender e participar em processos de gerenciamento de mudança

7.10 Implementar estratégias de recuperação

- Estratégias de armazenamento de backup
- Estratégias de recuperação de sites
- Múltiplos sites de processamento
- Resiliência do sistema, alta disponibilidade (HA), Qualidade de Serviço (QoS) e tolerância a falhas

7.11 Implementar processos de Recuperação de Desastres (DR)

- Resposta
- Equipa
- Comunicações
- Avaliação
- Restauração
- Treinamento e conhecimento
- Lições aprendidas

7.12 Teste de Planos de Recuperação de Desastre (DRP)

- Read-through/tabletop
- Passo a passo
- Simulação
- Paralelo
- Interrupção total

7.13 Participar no planejamento e exercícios de Continuidade de Negócios (BC)

7.14 Implementar e gerenciar segurança física

- Controles de segurança de perímetro
- Controles de segurança internos

7.15 Abordar preocupações com proteção e segurança pessoal

- Viagem
- Treinamento e conhecimento em Segurança
- Gerenciamento de emergência
- Coação

Domínio 8: Segurança no Desenvolvimento de Software

8.1 Compreender e integrar a segurança no Ciclo de Vida de Desenvolvimento de Software (SDLC)

- Metodologias de desenvolvimento (por exemplo, Agile, Waterfall, DevOps, DevSecOps)
- Modelos de maturidade (por exemplo, modelo de maturidade de capacidade (CMM), Software Assurance Maturity Model (SAMM))
- Operação e manutenção
- Gerenciamento de mudança
- Equipe de Produto Integrada (IPT)

8.2 Identificar e aplicar controles de segurança em ecossistemas de desenvolvimento de software

- Linguagens de programação
- Bibliotecas
- Conjuntos de ferramentas
- Ambiente de desenvolvimento integrado (IDE)
- Tempo de execução
- Integração Contínua e Entrega Contínua (CI/CD)
- Orquestração, Automação e Resposta de Segurança (SOAR)
- Gestão de Configuração de Software (SCM)
- Repositórios de código
- Teste de segurança de aplicativos (por exemplo, teste de segurança de aplicativo estático (SAST), teste de segurança de aplicativos dinâmicos (DAST))

8.3 Avaliar a eficácia da segurança do software

- Auditoria e registro de mudanças
- Análise e mitigação de riscos

8.4 Avaliar o impacto de segurança do software adquirido

- Comercial de prateleira (COTS)
- Código aberto
- Terceiros
- Sistemas gerenciados (por exemplo, Software Como Serviço (SaaS), Infraestrutura Como Serviço (IaaS), Plataforma como serviço (PaaS))

8.5 Definir e aplicar diretrizes e padrões de codificação seguros

- Fraquezas e vulnerabilidades de segurança no nível do código-fonte
- Segurança das Interfaces de Programação de Aplicativos (APIs)
- Práticas de codificação seguras
- Segurança Definida por Software

Informações Adicionais do Exame

Referências Suplementares

Os candidatos são encorajados a complementar sua educação e experiência revisando os recursos relevantes que pertencem ao CBK e identificando áreas de estudo que possam precisar de atenção adicional.

Veja a lista completa de referências suplementares em www.isc2.org/certifications/References.

Políticas e Procedimentos do Exame

(ISC)² recomenda que os candidatos ao CISSP revejam as políticas e procedimentos do exame antes de se inscreverem. Leia a análise abrangente dessas informações importantes em www.isc2.org/Register-for-Exam.

Informações Legais

Para quaisquer questões relacionadas apolíticas legais do (ISC)², entre em contato com o Departamento Legal do (ISC)² em legal@isc2.org.

Perguntas?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.866.331.ISC2 (4722)
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org