CISSP®

Certified Information Systems Security Professional

Sumário do Exame de Certificação

Data Efetiva: Abril de 2018

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

Sobre o CISSP

O Certified Information Systems Security Professional (CISSP) é a certificação globalmente mais reconhecida no mercado de segurança da informação. O CISSP valida o profundo conhecimento técnico e de gestão de um profissional de segurança da informação e sua experiência para efetivamente projetar, construir e gerenciar a postura geral de segurança de uma organização.

O amplo espectro de tópicos incluídos no Conjunto Comum de Conhecimentos (do inglês, CBK - Common Body of Knowledge) assegura sua relevância em todas as disciplinas no campo da segurança da informação. Candidatos bem-sucedidos são proficientes nos 8 seguintes domínios:

- Segurança e Gerenciamento de Riscos
- Segurança de Ativos
- Arquitetura e Engenharia de Segurança
- Segurança de Comunicação e Rede
- Gerenciamento de Identidade e Acesso (IAM)
- Avaliação e Teste de Segurança
- Operações de Segurança
- Segurança de Desenvolvimento de Software

Requisitos de Experiência

Os candidatos devem ter um mínimo de 5 anos de experiência acumulada de trabalho em período integral remunerado em 2 ou mais dos 8 domínios do CISSP CBK. Ter obtido um diploma de nível superior de 4 anos ou equivalente regional ou, uma credencial adicional da lista aprovada do (ISC)² cumprir com 1 ano da experiência requerida. O crédito educacional irá cumprir apenas com 1 ano de experiência.

Um candidato que não possuir a experiência exigida para se tornar um CISSP poderá se tornar um Associate do (ISC)² passando com sucesso no exame CISSP. O Associate do (ISC)² terá então 6 anos para obter os 5 anos de experiência exigidos.

Acreditação

O CISSP foi a primeira credencial no campo da segurança da informação a cumprir com os rigorosos requisitos da ANSI/ ISO/IEC Standard 17024.

Análise das Tarefas de Trabalho (JTA)

O (ISC)² tem uma obrigação 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 definhada pelo CISSP. Os resultados do JTA são usados para atualizar o exame. Este processo assegura que candidatos sejam testados nas áreas temáticas relevantes para os papéis e responsabilidades dos atuais profissionais praticantes da segurança da informação.

Informações Sobre o Exame CISSP CAT

O exame 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. Você pode aprender mais sobre CISSP CAT em www.isc2.org/certificatons/CISSP-CAT.

Duração do exame	3 horas
Número de questões	100 - 150
Formato das questões	Múltipla escolha e questões inovadoras avançadas
Nota de aprovação	700 de 1000 pontos
Idiomas disponíveis para exame	Inglês
Centros de testes	Centros de Testes Autorizados (ISC)2 da Pearson VUE PPC e PVTC Selecionados

Pesos do Exame CISSP CAT

Domínios	Peso Médio
1. Segurança e Gerenciamento de Riscos	15%
2. Segurança de Ativos	10%
3. Arquitetura e Engenharia de Segurança	13%
4. Segurança de Comunicação e Rede	14%
5. Gerenciamento de Identidade e Acesso (IAM)	13%
6. Avaliação e Teste de Segurança	12%
7. Operações de Segurança	13%
8. Segurança de Desenvolvimento de Software	10%
Total:	**100%**

Informações sobre o Exame Linear CISSP

Duração do exame	6 horas
Número de questões	250
Formato das questões	Múltipla escolha e questões inovadoras avançadas
Nota de aprovação	700 de 1000 pontos
Idiomas disponíveis para exame	Francês, Alemão, Português do Brasil, Espanhol, Japonês, Chinês Simplificado, Coreano
Centros de testes	Centros de Testes Autorizados (ISC)2 da Pearson VUE PPC e PVTC Selecionados

Pesos do Exame Linear CISSP

Domínios	Peso
1. Segurança e Gerenciamento de Riscos	15%
2. Segurança de Ativos	10%
3. Arquitetura e Engenharia de Segurança	13%
4. Segurança de Comunicação e Rede	14%
5. Gerenciamento de Identidade e Acesso (IAM)	13%
6. Avaliação e Teste de Segurança	12%
7. Operações de Segurança	13%
8. Segurança de Desenvolvimento de Software	10%
Total:	**100%**

Domínio 1: Segurança e Gerenciamento de Riscos

1.1 Entender e aplicar conceitos de confidencialidade, integridade e disponibilidade

1.2 Avaliar e aplicar princípios de governança de segurança

- Alinhamento da função de segurança com estratégia, metas, missão e objetivos do negócio
- Processos organizacionais (p.ex., aquisições, desinvestimentos, comitês de governança)
- Papeis e responsabilidades organizacionais
- Frameworks de controle de segurança
- Devido cuidado/devida diligência

1.3 Determinar requisitos de conformidade

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

1.4 Entender questões legais e regulatórias que se referem a segurança da informação em um contexto global

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

1.5 Entender, aderir e promover ética profissional

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

1.6 Desenvolver, documentar e implementar políticas de segurança, normas, procedimentos e guias

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

- Desenvolver e documentar escopo e planejamento
- Análise de Impacto no Negócio (AIN)

1.8 Contribuir e reforçar políticas e procedimentos de segurança de pessoal

- Seleção e contratação de candidatos
- Contratos e políticas de emprego
- Processos de integração e rescisão
- Contratos e controles de fornecedor, consultores e terceirizados
- Requisitos de política de conformidade
- Requisitos de política de privacidade

1.9 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 de Segurança (SCA)
- Monitoramento e medição
- Valoração de ativos
- Relatório
- Melhoria contínua
- Frameworks de riscos

1.10 Entender e aplicar conceitos e metodologias de modelagem de ameaças

- Metodologias de modelagem de ameaças
- Conceitos de modelagem de ameaças

1.11 Aplicar conceitos de gerenciamento baseados em risco à cadeia de suprimentos

- Riscos Associados com hardware, software e serviços
- Avaliação e monitoramento de terceiros
- Requisitos de segurança mínima
- Requisitos de nível de serviço

1.12 Estabelecer e manter um programa de conscientização, educação e capacitação em segurança

- Métodos e técnicas para conscientização e capacitação
- Revisões periódicas de conteúdo
- Avaliação de efetividade do programa

Domínio 2: Segurança de Ativos

2.1 Identificar e classificar informações e ativos

- Classificação de dados
- Classificação de ativos

2.2 Determinar e manter propriedade de informações e ativos

2.3 Proteger a privacidade

- Proprietários de dados
- Processadores de dados
- Remanência de dados
- Limitação de coleta

2.4 Assegurar apropriada conservação de ativos

2.5 Determinar controles de segurança de dados

- Entender os estados dos dados
- Escopo e recorte
- Seleção de padrões
- Métodos de proteção de dados

2.6 Estabelecer requisitos de manuseio de informações e ativos

Domínio 3: Arquitetura e Engenharia de Segurança

3.1 Implementar e gerenciar processos de engenharia usando princípios de projeto seguro

3.2 Entender os conceitos fundamentais de modelos de segurança

3.3 Selecionar controles baseados em requisitos de segurança de sistemas

3.4 Entender as capacidades de segurança dos sistemas de informações (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 banco de dados
- Sistemas de criptografia
- Sistemas de Controle Industrial (ICS)
- Sistemas baseados em nuvem
- Sistemas distribuídos
- Internet das Coisas (IoT)

3.6 Avaliar e mitigar vulnerabilidades em sistemas baseados na web

3.7 Avaliar e mitigar vulnerabilidades em sistemas móveis

3.8 Avaliar e mitigar vulnerabilidades em dispositivos embarcados

3.9 Aplicar criptografia

- Ciclo de vida criptográfico (por ejemplo, gestión de claves, selección de algoritmos)
- Métodos criptográficos (por ejemplo, curvas elípticas simétricas, asimétricas)
- Infraestructura de clave pública (PKI)
- Métodos de gestión de claves
- Firmas digitales
- No repudio
- Integridad (por ejemplo, hashing)
- Comprender los métodos de ataques criptoanalíticos
- Gestión de derechos digitales (DRM)

3.10 Aplicar princípios de segurança a projeto de site e instalações

3.11 Implementar controles de segurança de site e instalações

- Instalações de armários de cabeamento/ distribuição intermediária
- Salas de servidores/datacenters
- Instalações de armazenamento de mídias
- Armazenamento de evidência
- Segurança de área restrita e de trabalho
- Utilidades e, Aquecimento, Ventilação e Ar-Condicionado (HVAC)
- Questões ambientais
- Prevenção, detecção e supressão de incêndio

Domínio 4: Segurança de Comunicação e Rede

4.1 Implementar princípios de projeto Seguro em arquiteturas de rede

- Modelos Open System Interconnection (OSI) e Transmission Control Protocol/Internet Protocol (TCP/IP)
- Redes Internet Protocol (IP)
- Implicações de protocolos multicamadas
- Protocolos de convergência
- Redes definidas por software
- Redes sem fio

4.2 Componentes de rede segura

- Operação de hardware
- Meios de transmissão
- Dispositivos de Controle de Acesso à Rede (NAC)
- Segurança de endpoint
- Redes de distribuição de conteúdo

4.3 Implementar canais de comunicação segura de acordo com o projeto

- Voz
- Colaboração multimídia
- Acesso remoto
- Comunicações de dados
- Redes virtualizadas

Domínio 5: Gerenciamento de Identidade e Acesso (IAM)

5.1 Controle de acesso físico e lógico aos ativos

- Informações
- Sistemas
- Dispositivos
- Instalações

5.2 Gerenciar identificação e autenticação de pessoas, dispositivos e serviços

- Implementação de gerenciamento de identidade
- Autenticação único fator/multifator
- Prestação de contas
- Gerenciamento de sessão
- Registro e comprovação de identidade
- Gerenciamento de Identidade Federado (FIM)
- Sistemas de gerenciamento de credenciais

5.3 Integrar identidade como um serviço terceirizado

- Interno
- Nuvem
- Federado

5.4 Implementar e gerenciar mecanismos de autorização

- Controle de Acesso Baseado no Papel (RBAC)
- Controle de acesso baseado em regras
- Controle de Acesso Mandatório (MAC)
- Controle de Acesso Discricionário (DAC)
- Controle de Acesso Baseado em Atributo (ABAC)

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

- Revisão de acesso de usuário
- Revisão de acesso de conta de sistema
- Aprovisionamento e desaprovisionamento

Domínio 6: Avaliação e Teste de Segurança

6.1 Projetar e validar estratégias de avaliação, teste e auditoria

- Interna
- Externa
- Terceirizada

6.2 Conduzir testes de controle de segurança

- Avaliação de vulnerabilidades
- Testes de penetração
- Revisão de registros (logs)
- Transações sintéticas
- Revisão e testes de código
- Testes de caso de mau uso
- Análise de cobertura de teste
- Testes de interface

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

- Gerenciamento de conta
- Revisão e aprovação da gestão
- Indicadores chave de desempenho e risco
- Dados de verificação de backup
- Treinamento e conscientização
- Recuperação de Desastre (DR) e Continuidade de Negócios (BC)

6.4 Analisar resultados de teste e gerar relatório

6.5 Conduzir ou facilitar auditorias de segurança

- » Interna
- Externa
- Terceirizada

Domínio 7: Operações de Segurança

7.1 Entender e apoiar investigações

- Coleta e manuseio de evidência
- Relatórios e documentação
- Técnicas de investigação
- Ferramentas, táticas e procedimentos de forense digital

7.2 Entender requisitos por tipo de investigação

- Administrativa
- Criminal
- Cível
- Regulatória
- Padrões industriais

7.3 Conduzir atividades de registro e monitoramento

- Detecção e prevenção de intrusão
- Gerenciamento de segurança da informação e eventos (SIEM)
- Monitoramento contínuo
- Monitoramento de saída

7.4 Aprovisionamento seguro de recursos

- Inventário de ativos
- Gerenciamento de ativos
- Gerenciamento de configuração

7.5 Entender e aplicar conceitos fundamentais de segurança de operações

- Necessidade de conhecimento/privilégios mínimos
- Separação de deveres e responsabilidades
- Gerenciamento de contas privilegiadas
- Rotação de funções
- Ciclo de vida de informações
- Acordos de nível de serviço (SLA)

7.6 Aplicar técnicas de proteção de recursos

- Gerenciamento de mídias
- Gerenciamento de ativos de hardware e software

7.7 Conduzir gerenciamento de incidentes

- Detecção
- Resposta
- Mitigação
- Relatório
- Recuperação
- Remediação
- Lições aprendidas

7.8 Operar e manter medidas de detecção e prevenção

- Firewalls
- Intrusion detection and prevention systems
- Listas brancas/listas negras
- Serviços de segurança providos por terceiros
- Sandboxing
- Honeypots/honeynets
- Anti-malware

7.9 Implementar e suportar gerenciamento de patch e vulnerabilidade

7.10 Entender e participar em processos de gerenciamento de mudança

7.11 Implementar estratégias de recuperação

- Estratégias de armazenamento de backup
- Estratégias de site de recuperação
- Múltiplos sites de processamento
- Resiliência sistêmica, alta disponibilidade, Qualidade de Serviço (QoS) e tolerância a falha

7.12 Implementar processos de Recuperação de Desastres

- Resposta
- Pessoal
- Comunicações
- Assessment
- Restauração
- Treinamento e conscientização

7.13 Testar Planos de Recuperação de Desastre (DRP)

- Teste de leitura / teste de mesa
- Passo a passo
- Simulação
- Paralelo
- Interrupção total

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

7.15 Implementar e gerenciar segurança física

- Controles de segurança de perímetro
- Controles de segurança interna

7.16 Endereçar preocupações com proteção e segurança pessoal

- Viagem
- Treinamento e conscientização em segurança
- Gerenciamento de emergência
- Prisão

Domínio 8:
Segurança de Desenvolvimento de Software

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

- Metodologias de desenvolvimento
- Modelos de maturidade
- Operação e manutenção
- Gerenciamento de mudanças
- Equipe de produtos integrados

8.2 Identificar e aplicar controles de segurança em ambientes de desenvolvimento

- Segurança de ambientes de software
- Gerenciamento de configuração como um aspecto de segurança de codificação
- Segurança dos repositórios de código

8.3 Avaliar a eficácia da segurança de software

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

8.4 Avaliar impacto de segurança de software adquirido

8.5 Definir e aplicar guias e padrões de codificação segura

- Fragilidades e vulnerabilidades de segurança no nível de código-fonte
- Segurança das interfaces dos aplicativos de programação
- Práticas de codificação segura

Informações Adicionais de Exame

Referências Suplementares

Os candidatos são incentivados a complementar sua educação e experiência com a revisão de recursos relevantes que dizem respeito ao CBK e identificarem áreas de estudo que possam necessitar de atenção adicional.

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

Políticas e Procedimentos de Exame

O (ISC)² recomenda que candidatos ao CISSP revisem as políticas e procedimentos de exame antes de se inscrever para o exame. Leia um abrangente detalhamento destas importantes informações em www.isc2.org/Register-for-Exam.

Informações Legais

Para qualquer questão relacionada às políticas legais do (ISC)², por favor, contate o (ISC)2 Legal Department em legal@isc2.org.

Alguma pergunta?

(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