# Cybersecurity Essentials 1.0
# Escopo e sequência

**Última atualização 4 de janeiro de 2018**

## Público-alvo

O cu*rso Cybersecurity Essentials 1.0* foi criado para alunos que estão interessados na busca de estudos mais avançados no campo da segurança cibernética. Esse curso preparatório dá uma visão geral do campo da segurança cibernética. A grade curricular explora as características dos criminosos virtuais e as táticas usadas por eles. Em seguida, destrincha as tecnologias, produtos e procedimentos que o profissional da segurança cibernética usa para combater o crime digital. O currículo é apropriado para alunos em vários níveis de educação e tipos de instituições, incluindo escolas de ensino médio, universidades, faculdades, escolas profissionais e técnicas, bem como centros comunitários.

## Pré-requisitos

Para moldar qualificações profissionais adequadas, os alunos devem estar familiarizados com o conteúdo e as qualificações profissionais descritas nos pré-requisitos do curso:

- Introdução ao Cybersecurity 2.0

## Certificações Alvo

Não há certificações alvo para este curso

## Descrição do Currículo

O curso dispõe de muitos recursos que ajudam os alunos a entender esses conceitos:

- Conteúdo multimídia avançado, como atividades interativas, vídeos, jogos e testes, para atender a estilos de aprendizagem variados, ajudar a estimular o aprendizado e aumentar a retenção do conhecimento
- Os laboratórios práticos e as atividades de aprendizado baseadas na simulação do Packet Tracer ajudam os alunos a desenvolver atividades de pensamento crítico e de solução de problemas complexos
- Análises inovadoras oferecem feedback imediato para dar respaldo às avaliações de conhecimento e habilidades adquiridas
- Os conceitos técnicos são explicados com uma linguagem apropriada para estudantes de todos os níveis e as atividades interativas integradas dividem a leitura do conteúdo em partes e reforçam o entendimento
- A grade curricular incentiva os alunos a pensarem em se aprofundar academicamente em TI e também enfatiza as qualificações profissionais aplicadas e a experiência prática

As atividades do Cisco Packet Tracer foram elaboradas para o Packet Tracer 6.3 ou versão mais recente.

## Objetivos do Currículo

O *Cybersecurity Essentials 1.0* abrange o conhecimento dos fundamentos e as qualificações profissionais essenciais em todos os domínios da segurança: segurança da informação, segurança de sistemas, segurança de rede, segurança móvel, segurança física, ética e leis e tecnologias relacionadas, além do uso de técnicas de defesa e de mitigação na proteção das empresas.

Depois da conclusão do curso *Cybersecurity Essentials 1.0*, os alunos serão capazes de realizar as seguintes tarefas:

- Descrever as características dos criminosos e heróis no campo da segurança cibernética.
- Descrever os princípios de confidencialidade, integridade e disponibilidade, conforme eles se relacionam aos estados dos dados e às contramedidas de segurança cibernética.
- Descrever as táticas, técnicas e procedimentos usados por criminosos virtuais.
- Descrever como as tecnologias, produtos e procedimentos são usados para proteger a confidencialidade.
- Descrever como as tecnologias, produtos e procedimentos são usados para garantir a integridade.
- Descrever como as tecnologias, produtos e procedimentos fornecem a alta disponibilidade.
- Explicar como os profissionais da segurança cibernética usam tecnologias, processos e procedimentos para defender todos os componentes da rede.
- Explicar a finalidade das leis relacionadas à segurança cibernética.

## Requisitos Mínimos de Sistema

Para uma experiência de aprendizado melhor, recomendamos o número de 12 a 15 alunos na turma, na proporção de um computador de laboratório por aluno. Nos laboratórios práticos, no máximo dois alunos podem compartilhar um computador. Algumas atividades de laboratório exigem que os computadores do laboratório estejam conectados a uma rede local.

## Requisitos de Hardware dos PCs de Laboratório

- Computador com um mínimo de 2 GB de RAM e 8 GB de espaço livre em disco
- Acesso à Internet de alta velocidade para baixar o Oracle VirtualBox e o arquivo de imagem de máquina virtual

## Visão Geral do Grau Curricular

O *Cybersecurity Essentials 1.0* ajuda os alunos:

- A entender os participantes do mundo da segurança cibernética e a motivação dos criminosos virtuais e dos especialistas em segurança cibernética.
- A aprender a identificar ataques à segurança, sintomas, processos e contramedidas.
- A ter o conhecimento dos fundamentos em vários domínios de segurança.
- A construir as qualificações profissionais nas tecnologias de gerenciamento, controles, proteção e mitigação da segurança.
- A aprender as leis de segurança, de ética e de como desenvolver as políticas de segurança.
- A aprender as funções de diferentes profissionais de segurança cibernética e as opções de carreira.

## Estrutura do curso

**Tabela 1.** Cybersecurity Essentials 1.0 Descrição do curso

| Capítulo/Seção | Metas/Objetivos |
|---|---|
| **Capítulo 1. Segurança cibernética: Um mundo de magia, criminosos e heróis** | **Descreve as características dos criminosos e heróis no ambiente de segurança cibernética.** |
| 1.1 O mundo da segurança cibernética | Descreve as características comuns que compõem o mundo da segurança cibernética |
| 1.2 Criminosos virtuais contra os heróis virtuais | Diferencia as características dos criminosos e dos heróis virtuais. |
| 1.3 As ameaças ao reino | Compara como as ameaças à segurança cibernética afetam indivíduos, empresas e organizações. |
| 1.4 As forças das trevas da segurança cibernética | Descreve os fatores que levam à propagação e crescimento de crimes digitais. |
| 1.5 Criação de mais heróis | Descreve as organizações e os esforços empenhados em expandir a força de trabalho da segurança cibernética. |
| **Capítulo 2. O cubo de feitiçaria da segurança cibernética** | **Descreve os princípios de confidencialidade, integridade e disponibilidade, conforme eles se relacionam aos estados dos dados e às contramedidas de segurança cibernética.** |
| 2.1 o cubo de feitiçaria de segurança cibernética | Descreve as três dimensões do cubo McCumber. |
| 2.2 Tríade CIA | Descreve os princípios de confidencialidade, integridade e disponibilidade. |
| 2.3 Os estados dos dados | Diferencia os três estados dos dados. |
| 2.4 Contramedidas de segurança cibernética | Compara os tipos de contramedidas de segurança cibernética. |
| 2.5 Estrutura de gerenciamento de segurança da TI | Descreve o modelo de segurança cibernética ISO |
| **Capítulo 3. Ameaças, vulnerabilidades e ataques à segurança cibernética** | **Descreve as táticas, técnicas e procedimentos usados por criminosos virtuais.** |
| 3.1 Malware e código malicioso | Diferencia os tipos de malware e código malicioso. |
| 3.2 Artifícios | Compara os diferentes métodos usados em social engineering. |
| 3.3 Ataques | Compara diferentes tipos de ataques cibernéticos. |
| **Capítulo 4. A arte de proteger segredos** | **Descreve como as tecnologias, produtos e procedimentos são usados para proteger a confidencialidade.** |
| 4.1 criptografia | Explica como as técnicas de criptografia protegem a confidencialidade. |
| 4.2 Controles de acesso | Descreve como técnicas de controle de acesso protegem a confidencialidade. |
| 4.3 Ocultar dados | Descreva o conceito de ofuscação de dados. |

| | |
|---|---|
| **Capítulo 5. A arte de garantir a integridade** | **Descreve como as tecnologias, produtos e procedimentos são usados para garantir a integridade.** |
| 5.1 Tipos de controle de integridade de dados | Explica os processos usados para garantir a integridade. |
| 5.2 Assinaturas digitais | Explica a finalidade das assinaturas digitais. |
| 5.3 Certificados | Explica a finalidade dos certificados digitais. |
| 5.4 Reforço de integridade do banco de dados | Explica a necessidade do reforço na integridade do banco de dados. |
| **Capítulo 6. O reino dos cinco noves** | **Descreve como as tecnologias, produtos e procedimentos fornecem a alta disponibilidade.** |
| 6.1 Alta disponibilidade | Explica o conceito de alta disponibilidade. |
| 6.2 Medidas para melhorar a disponibilidade | Explica como as medidas de alta disponibilidade são usadas para melhorar a disponibilidade. |
| 6.3 Resposta a incidente | Descreve como um plano de resposta a incidente melhora a alta disponibilidade. |
| 6.4 Recuperação de desastres | Descreve como o planejamento de recuperação de desastres tem uma função importante na implementação da alta disponibilidade. |
| **Capítulo 7. Fortalecer o reino** | **Explica como os profissionais da segurança cibernética usam tecnologias, processos e procedimentos para defender todos os componentes da rede.** |
| 7.1 Defender sistemas e dispositivos | Explica como os processos e procedimentos protegem os sistemas. |
| 7.2 Blindagem do servidor | Explica como proteger os servidores em uma rede. |
| 7.3 Blindagem da rede | Explique como implementar as medidas de segurança para proteger os dispositivo de rede. |
| 7.4 Segurança física e ambiental | Explica como as medidas de segurança física são implementadas para proteger o equipamento da rede. |
| **Capítulo 8. Juntar-se a ordem dos heróis virtuais** | **Explica a finalidade das leis relacionadas à segurança cibernética.** |
| 8.1 Domínios da segurança cibernética | Descreve como os domínios da segurança cibernética são usados dentro da tríade CIA. |
| 8.2 Noções básicas sobre o juramento de adesão | Explica como a ética fornece orientação. |
| 8.3 Próximo passo | Explica como dar o próximo passo para se tornar um profissional da segurança cibernética |


Sede - América
Cisco Systems. Inc
San Jose. CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pad Ltd.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdam,
Países Baixos

A Cisco possui mais de 200 escritórios no mundo todo. Os endereços, números de telefones e fax estão disponíveis no site **www.cisco.com/go/offices**.