# Laboratório — Identificação de Ameaças

## Objetivos

Explore os recursos de segurança usados pelas organizações para garantir a segurança dos dados.

**Parte 1: Explorando a Ameaça dos Ciberataques**

**Parte 2: A Tríade CIA**

## Contexto/cenário

As ameaças colocadas pelo cibermundo são reais. Estas ameaças têm o potencial de causar estragos num mundo centrado em computadores. Compreender estas ameaças é importante para todos e, para combatê-las, são necessários indivíduos competentes que possam reconhecer e prever as ameaças, e superar os cibercriminosos. Para desenvolver o talento necessário, organizações como CompTIA, Cisco Systems e ISC2 criaram programas para educar e certificar profissionais em cibersegurança.

## Recursos necessários

- PC ou dispositivo móvel com acesso à Internet

# Parte 1: Explorando a Ameaça dos Ciberataques

Os ciberataques estão no topo da lista de ameaças em vários países. Quando se pensa em ameaças à segurança nacional ou mundial, a maioria das pessoas pensa em ataques físicos ou armas de destruição em massa. O facto é que as ciberameaças estão no topo da lista em mais de vinte países, globalmente. Os ciberataques classificados como mais relevantes revelam algumas coisas sobre como a sociedade mudou. Computadores e redes de computadores afetaram a maneira como aprendemos, compramos, comunicamos, viajamos e vivemos. Os computadores influenciam muitos aspetos das nossas vidas. A perturbação de computadores e redes de computadores pode ter um impacto devastador na vida das pessoas. Sistemas de geração e distribuição de energia elétrica, sistemas de tratamento e abastecimento de água, transporte e sistemas financeiros são alvos de ciberataques. Cada um destes sistemas foi vítima de ciberataques. Observe o vídeo abaixo. Crie grupos de 3-4 pessoas. Depois de visualizar o vídeo, responda às perguntas abaixo.

### Passo 1: Pesquisa de Ameaças.

No passo 1, serão pesquisadas ameaças.

a. Clique aqui para ver o vídeo. De acordo com o vídeo, qual é a arma mais perigosa do mundo? Porquê? Concorda?

_____

_____

b. Liste cinco métodos usados por um cibercriminoso para violar a lei. Algum dos crimes listados pode afetá-lo pessoalmente? Você ou seus familiares alguma vez foram afetados por este tipo de crimes?

_____

_____

c. Alguma das possíveis ameaças retratadas no vídeo aconteceu na realidade? Clique aqui para aprender mais sobre estes ataques.

_____

_____

### Passo 2: Explore Ataques Recentes.

a. O impacto e a abrangência de ciberataques recentes têm preocupado muitas empresas e governos. Clique aqui para rever o top 10 hacks cibernéticos mais devastadores de 2015.

Quantas pessoas foram afetadas pela violação de dados do *US Office of Personnel Management*?

_____

_____

b. Descreva o ataque TalkTalk de 2015. Quem foi o responsável e o que foi roubado pelos cibercriminosos?

_____

_____

## Parte 2: Tríade CIA

Confidencialidade, integridade e disponibilidade (do termo inglês *accounting*) são os três princípios fundamentais de cibersegurança. Estes três princípios compõem a tríade CIA. Os elementos da tríade são os três componentes mais cruciais da segurança. Todos os profissionais de cibersegurança devem estar familiarizados com esses princípios fundamentais.

### Passo 1: Explore a Tríade CIA

a. Clique aqui para ver o vídeo. O que é a confidencialidade dos dados? Por que motivo a confidencialidade dos dados é tão importante para pessoas e organizações?

_____

_____

b. O que é a integridade dos dados? Indique três formas de afetar a integridade ou a confiança dos dados.

_____

_____

c. O que é a disponibilidade de um sistema? O que pode acontecer se um computador, considerado crítico, ficar indisponível?

_____

_____

### Passo 2: Explore os Ciberataques.

Clique aqui para assistir a um vídeo. Qual era o objetivo dos cibercriminosos? A que horas do dia ocorreu o ataque? É provável que os ataques de rede ocorram fora de horas? Porquê?

_____

_____