

## Microsoft® Windows® Security

### Objetivos Gerais

Este Curso é dirigido a todos os profissionais envolvidos na gestão, implementação e manutenção da Segurança dos Sistemas Windows.

### Objetivos Específicos

No final do Curso os formandos ficaram aptos:

- A dominar o básico de segurança em um ambiente Microsoft;
- Dominar os objetivos da certificação de fundamentos de segurança do Microsoft tecnologia Associate (MTA);
- Compreender as camadas de segurança;
- Entender a segurança do sistema operacional;
- Entender a segurança da rede;
- Entender o software de segurança;
- Dominar todos os objetivos do Microsoft Technology Associate Security Fundamentals exam (exam 98-367).

### Destinatários

Este Curso destina-se a todos os profissionais que necessitem dos fundamentos da segurança num ambiente Microsoft. O objetivo é fornecer uma cobertura rápida e focada dos Skills fundamentais de segurança.

### Pré-requisitos

Os pré-requisitos necessários para frequentar este curso são:

- Ter acesso a um computador ou um tablet com ligação à Internet e um browser (programa para navegar na web), como o Chrome, Safari, Firefox ou Internet Explorer.
- Pode aceder ao curso a partir de qualquer computador (por exemplo, em casa e no escritório), tablet ou smartphone.

### Carga Horária

40 Horas

### Conteúdo Programático

#### Módulo 0 – Apresentação de Plataforma e Método de Utilização

#### Módulo I – Understanding Core Security Principles

- Understanding Risk
- Exploring the Security Triad
- Implementing a Defense-in-Depth Security Strategy

- Enforcing the Principle of Least Privilege
- Hardening a Server

## **Módulo II – Understanding Malware and Social Engineering**

- Comparing Malware
- Protecting Against Malware
- Thwarting Social-Engineering Attacks
- Protecting Email

## **Módulo III - Understanding User Authentication**

- Comparing the Three Factors of Authentication
- Using Passwords for Authentication
- Using Smart Cards and Token Devices for Authentication
- Using Biometrics for Authentication
- Starting Applications with Run As Administrator
- Preventing Time Skew with Kerberos
- Identifying RADIUS Capabilities
- Identifying Unsecure Authentication Protocols

## **Módulo IV - Securing Access with Permissions**

- Comparing NTFS Permissions
- Exploring Share Permissions
- Identifying Active Directory Permissions
- Assigning Registry Permissions

## **Módulo V - Using Audit Policies and Network Auditing**

- Exploring Audit Policies
- Enabling Auditing
- Viewing Audit Information
- Managing Security Logs
- Auditing a Network with MBSA

## **Módulo VI - Protecting Clients and Servers**

- Understanding User Account Control
- Keeping Systems Updated
- Protecting Clients
- Protecting Servers
- Exploring DNS Security Issues

### **Módulo VII - Protecting a Network**

- Identifying Common Attack Methods
- Exploring Firewalls
- Exploring Network Access Protection
- Identifying Protocol Security Methods

### **Módulo VIII - Understanding Wireless Security**

- Comparing Wireless Devices
- Comparing Wireless Security Methods
- Configuring Wireless Routers
- Configuring Windows 7 for Wireless

### **Módulo IX - Understanding Physical Security**

- Comparing Site Security and Computer Security
- Using Group Policy to Enhance Computer Security
- Exploring Mobile Device Security

### **Módulo X - Enforcing Confidentiality with Encryption**

- Comparing Encryption Methods
- Securing Email
- Understanding EFS
- Exploring BitLocker Drive Encryption

### **Módulo XI - Understanding Certificates and a PKI**

- Understanding a Certificate
- Exploring the Components of a PKI

### **Módulo XII - Understanding Internet Explorer Security**

- Exploring Browser Settings
- Comparing Security Zones
- Using IE Tools to Identify Malicious Websites

## **Metodologia**

Este curso tem sempre presente o formador, que irá mesmo dar a formação presencial através da plataforma.

O Formando pode intervir juntamente com o formador ou com os restantes formandos tal como faz na sala de aula.

As apresentações e exercícios serão sempre disponibilizados pelo formador no final de cada sessão de formação.

No final do curso receberá um Certificado de Formação Profissional caso frequente pelo menos 90% das aulas, realize os trabalhos e os testes propostos, participe nas discussões online e tenha avaliação final positiva.

Esta formação é certificada e reconhecida.