IMECAF®

www.imecaf.com

CURSO DE SEGURIDAD INFORMÁTICA

TI

INVERSIÓN
$5,829.00 + IVA

DURACIÓN
90 HRS.

MODALIDAD
En Linea

Tel. 55 1085 1515 / 800 236 0800 | info@imecaf.com

CURSO DE SEGURIDAD INFORMÁTICA

TI

OBJETIVO

El curso de Seguridad Informática TestOut Security Pro prepara a los estudiantes para el examen de certificación TestOut Security Pro y el examen de certificación CompTIA Security + SY0-401. Los estudiantes aprenden cómo proteger una red corporativa usando un modelo de seguridad en capas.

DIRIGIDO A

Este curso de Seguridad Informática va dirigido a toda persona que quiera obtener la certificación CompTIA Security+ SY0-401 o que busque convertirse en un especialista en seguridad, para desempeñar mejor sus funciones como administrador o encargado de sistemas de TI.

CURSO DE SEGURIDAD INFORMÁTICA

TI

BENEFICIOS

Aprobado por CompTIA

TestOut Security Pro posee contenido de calidad aprobado por CompTIA y se ha verificado que cubre el 100 % de los objetivos del examen de certificación CompTIA Security+ SY0-401.

Simulaciones de la vida real

LabSim imita $35 000 USD en hardware y software informático y desafía a los estudiantes con escenarios del mundo real. Los estudiantes que completan el curso están preparados con el conocimiento y las habilidades que necesitan para ser un exitoso administrador de seguridad de TI.

Enfoque de seguridad en capas

TestOut Security Pro enseña a los estudiantes cómo proteger correctamente una red usando un modelo de seguridad en capas. Los estudiantes aprenden y luego construyen una red segura, comenzando por medidas de seguridad física y progresando hasta las defensas de datos, al igual que harían en el trabajo.

Múltiples sistemas operativos

Durante el curso, los estudiantes adquieren experiencia con múltiples sistemas operativos e interfaces como Windows 7 Ultimate, Windows Server 2012 R2 Datacenter, iOS, Cisco CLI (enrutadores y conmutadores), Cisco Net Security Appliance y Linux CLI.

Exámenes ilimitados de práctica de certificación

TestOut Security Pro incluye exámenes de práctica para el examen de certificación TestOut Security Pro y el examen de certificación CompTIA Security+ SY0-401. Los estudiantes pueden adquirir confianza y habilidades de prueba al practicar todas las veces que lo deseen.

TEMARIO

CURSO DE SEGURIDAD INFORMÁTICA

TI

I. INTRODUCTION

a. Security Overview

i. Security Challenges (8:22)
ii. Security Roles and Concepts (5:37)
iii. Threat Agent Types (8:20)
iv. Security Introduction
v. General Attack Strategy (8:51)
vi. General Defense Strategy (18:25)
vii. Attack and Defense Strategy Overview
viii. Practice Questions - Section 1.1

b. Using the Simulator

i. Using the Simulator (13:19)
ii. Configure a Security Appliance
iii. Install a Security Appliance

II. ACCESS CONTROL AND IDENTITY MANAGEMENT

a. Access Control Models

i. Access Control Models (3:38)
ii. Access Control Facts
iii. Access Control Model Facts
iv. Access Control Model Examples
v. Implementing Discretionary Access Control (6:09)
vi. Practice Questions - Section 2.1

b. Authentication

i. Authentication Part 1 (11:26)
ii. Authentication Part 2 (8:53)
iii. Authentication Facts
iv. Using a Biometric Scanner (3:49)
v. Using Single Sign-on (12:20)

vi. Single Sign-on Facts
vii. Practice Questions - Section 2.2

c. **Authorization**
   i. Authorization (5:15)
   ii. Cumulative Access (9:32)
   iii. Authorization Facts
   iv. Examining the Access Token (9:08)
   v. Practice Questions - Section 2.3

d. **Access Control Best Practices**
   i. Access Control Best Practices (3:12)
   ii. Viewing Implicit Deny (10:13)
   iii. Best Practices Facts
   iv. Practice Questions - Section 2.4

e. **Active Directory Overview**
   i. Active Directory Introduction (9:04)
   ii. Active Directory Structure (9:25)
   iii. Viewing Active Directory (8:05)
   iv. Active Directory Facts
   v. Practice Questions - Section 2.5

f. **Windows Domain Users and Groups**
   i. Creating User Accounts (4:50)
   ii. Managing User Account Properties (7:45)
   iii. Create User Accounts
   iv. Manage User Accounts
   v. Managing Groups (5:05)
   vi. Create a Group
   vii. Create Global Groups
   viii. User Account Management Facts
   ix. Practice Questions - Section 2.6

g. **Linux Users**

i. Linux User and Group Overview (19:14)
ii. Managing Linux Users (9:28)
iii. Linux User Commands and Files
iv. Create a User Account
v. Rename a User Account
vi. Delete a User
vii. Change Your Password
viii. Change a User´s Password
ix. Lock and Unlock User Accounts
x. Practice Questions - Section 2.7

h. **Linux Groups**
   i. Managing Linux Groups (3:15)
   ii. Linux Group Commands
   iii. Rename and Create Groups
   iv. Add Users to a Group
   v. Remove a User from a Group
   vi. Practice Questions - Section 2.8

i. **Linux User Security**
   i. Linux User Security and Restrictions (9:53)
   ii. Configuring Linux User Security and Restrictions (6:40)
   iii. Linux User Security and Restriction Facts
   iv. Practice Questions - Section 2.9

j. **Group Policy Overview**
   i. Group Policy Overview (8:41)
   ii. Viewing Group Policy (14:31)
   iii. Group Policy Facts
   iv. Create and Link a GPO
   v. Practice Questions - Section 2.10

k. **Hardening Authentication 1**
   i. Hardening Authentication (19:31)
   ii. Configuring User Account Restrictions (9:30)

iii. Configure User Account Restrictions
iv. Configuring Account Policies and UAC Settings (14:18)
v. Configure Account Policies
vi. Hardening User Accounts (10:20)
vii. Restrict Local Accounts
viii. Secure Default Accounts
ix. Enforce User Account Control
x. Hardening Authentication Facts
xi. Practice Questions - Section 2.11

l. **Hardening Authentication 2**
   i. Configuring Smart Card Authentication (6:20)
   ii. Configure Smart Card Authentication
   iii. Smart Card Authentication Facts
   iv. Using Fine-Grained Password Policies (7:00)
   v. Fine-Grained Password Policy Facts
   vi. Create a Fine-Grained Password Policy
   vii. Practice Questions - Section 2.12

m. **Remote Access**
   i. Remote Access (8:44)
   ii. Remote Access Facts
   iii. RADIUS and TACACS+ (6:52)
   iv. RADIUS and TACACS+ Facts
   v. Practice Questions - Section 2.13

n. **Network Authentication**
   i. Network Authentication Protocols (14:09)
   ii. Network Authentication via LDAP (10:31)
   iii. Network Authentication Facts
   iv. Controlling the Authentication Method (6:39)
   v. Configure Kerberos Policy Settings
   vi. Browsing a Directory Tree via LDAP (6:38)
   vii. Trusts and Transitive Access (5:34)

viii. Trusts and Transitive Access Facts
ix. Credential Management (10:06)
x. Credential Management Facts
xi. Practice Questions - Section 2.14

o. **Identity Management**
   i. Identity Management (16:31)
   ii. Identity Management Facts
   iii. Practice Questions - Section 2.15

III. CRYPTOGRAPHY

a. **Cryptography**
   i. Cryptography Concepts (4:30)
   ii. Cryptography Facts
   iii. Cryptographic Attacks (17:48)
   iv. Cryptographic Attack Facts
   v. Practice Questions - Section 3.1

b. **Hashing**
   i. Hashing (11:31)
   ii. Hashing Facts
   iii. Using Hashes (7:43)
   iv. Practice Questions - Section 3.2

c. **Symmetric Encryption**
   i. Symmetric Encryption (5:27)
   ii. HMAC (6:14)
   iii. Symmetric Encryption Facts
   iv. Cracking a Symmetric Encryption Key (4:11)
   v. Practice Questions - Section 3.3

d. **Asymmetric Encryption**
   i. Asymmetric Encryption (8:14)
   ii. Asymmetric Encryption Facts
   iii. Practice Questions - Section 3.4

e. **Public Key Infrastructure (PKI)**
   i. Certificates (11:02)
   ii. Managing Certificates (14:45)
   iii. Manage Certificates
   iv. Certificate Lifecycle Facts
   v. CA Implementation (5:17)
   vi. Configuring a Subordinate CA (14:13)
   vii. PKI Management Facts
   viii. Practice Questions - Section 3.5

f. **Cryptography Implementations**
   i. Combining Cryptographic Methods (10:30)
   ii. Hardware Based Encryption Devices (7:13)
   iii. Cryptographic Implementation Facts
   iv. Practice Questions - Section 3.6

IV. POLICIES, PROCEDURES, AND AWARENESS

a. **Security Policies**
   i. Security Policies (7:23)
   ii. Data Privacy Laws (9:43)
   iii. Security Policy Facts
   iv. Security Documentation Facts
   v. Security Management Facts
   vi. Information Classification (5:40)
   vii. Information Classification Facts
   viii. Data Retention Policies (11:40)
   ix. Wiping a Hard Drive (12:58)
   x. Data Retention Facts
   xi. Practice Questions - Section 4.1

b. **Manageable Network Plan**
   i. Manageable Network Plan (16:49)
   ii. Manageable Network Plan 2 (14:05)

iii. Manageable Network Plan Facts
iv. Practice Questions - Section 4.2

c. **Business Continuity**
   i. Business Continuity (2:39)
   ii. Succession Planning (5:23)
   iii. Business Continuity Facts
   iv. Practice Questions - Section 4.3

d. **Risk Management**
   i. Risk Management (4:04)
   ii. Security Controls (3:21)
   iii. Data Loss Prevention (DLP) (4:57)
   iv. Risk Management Facts
   v. Practice Questions - Section 4.4

e. **Incident Response**
   i. First Responder (7:17)
   ii. Basic Forensic Procedures (18:31)
   iii. Using Forensic Tools (6:17)
   iv. Creating a Forensic Drive Image (10:00)
   v. Incident Response Facts
   vi. Forensic Investigation Facts
   vii. Practice Questions - Section 4.5

f. **Social Engineering**
   i. Social Engineering (4:40)
   ii. Phishing Variations (13:04)
   iii. Social Engineering Facts
   iv. Investigating a Social Engineering Attack (9:45)
   v. Respond to Social Engineering
   vi. Practice Questions - Section 4.6

g. **Certification and Accreditation**
   i. Trusted Computing (10:01)

ii. Certification and Accreditation (4:46)
iii. Certification and Accreditation Facts
iv. Practice Questions - Section 4.7

h. **Development**
   i. System Development Life Cycle (8:40)
   ii. System Development Life Cycle 2 (7:49)
   iii. SDLC Facts
   iv. Software Development Models
   v. Practice Questions - Section 4.8

i. **Employee Management**
   i. Employment Practices (13:45)
   ii. Employee Management Facts
   iii. Employee Documents Facts
   iv. Ethics Facts
   v. Practice Questions - Section 4.9

j. **Third-Party Integration**
   i. Third-Party Integration Security Issues (11:24)
   ii. Third-Party Integration Security Facts
   iii. Practice Questions - Section 4.10

V. PHYSICAL SECURITY

a. **Physical Security**
   i. Physical Security (18:39)
   ii. Tailgating and Piggybacking (3:28)
   iii. Physical Security Facts
   iv. Hardware Security
   v. Hardware Security Guidelines (7:50)
   vi. Breaking into a System (7:30)
   vii. Hardware Security Facts
   viii. Practice Questions - Section 5.2

b. **Environmental Controls**

i. Environmental Controls (6:00)
ii. Environmental Monitoring (11:33)
iii. Hot and Cold Aisles (5:17)
iv. Environmental Control Facts
v. Fire Protection Facts
vi. Practice Questions - Section 5.3

c. **Mobile Devices**
   i. Mobile Device Security (7:34)
   ii. Mobile Device Security Facts
   iii. BYOD Security Issues (9:33)
   iv. BYOD Security Facts
   v. Securing Mobile Devices (10:20)
   vi. Secure an iPad
   vii. Practice Questions - Section 5.4

d. **Mobile Device Security Enforcement**
   i. Enforcing Security Policies on Mobile Devices (7:57)
   ii. Enrolling Devices and Performing a Remote Wipe (8:49)
   iii. Mobile Device Security Enforcement Facts
   iv. Mobile Application Security (9:00)
   v. Mobile Application Security Facts
   vi. Practice Questions - Section 5.5

e. **Telephony**
   i. Telephony (15:00)
   ii. Telephony Security Facts
   iii. Practice Questions - Section 5.6

VI. **PERIMETER DEFENSES**

a. **Network Layer Protocol Review**
   i. OSI Model (4:08)
   ii. OSI Model Facts
   iii. IP Addressing (17:22)

IMECAF®

iv. IP Address Facts
v. Configuring IPv6 (5:28)
vi. IP Subnetting (12:35)
vii. Configuring Subnetting (8:07)
viii. Subnetting Facts
ix. Practice Questions - Section 6.1

b. **Transport Layer Protocol Review**
   i. Network Protocols (4:45)
   ii. Network Protocol Facts
   iii. Analyzing a TCP Three-way Handshake (2:14)
   iv. TCP and UDP Ports (9:02)
   v. Common Ports
   vi. Practice Questions - Section 6.2

c. **Perimeter Attacks 1**
   i. Reconnaissance (2:40)
   ii. Performing Reconnaissance (9:01)
   iii. Reconnaissance Facts
   iv. Denial of Service (DoS) (7:49)
   v. Xmas Tree Attacks (3:23)
   vi. DoS Attack Facts
   vii. Performing a UDP Flood Attack (3:54)
   viii. Practice Questions - Section 6.3

d. **Perimeter Attacks 2**
   i. Session and Spoofing Attacks (6:41)
   ii. Session Based Attack Facts
   iii. Performing ARP Poisoning (4:24)
   iv. Spoofing Facts
   v. DNS Attacks (4:30)
   vi. DNS Attack Facts
   vii. Examining DNS Attacks (13:29)
   viii. Prevent Zone Transfers

ix. Practice Questions - Section 6.4

e. **Security Appliances**
   i. Security Solutions (4:02)
   ii. Security Zones (5:32)
   iii. Security Zone Facts
   iv. All-In-One Security Appliances (4:30)
   v. Security Solution Facts
   vi. Configuring Network Security Appliance Access (6:55)
   vii. Configure Network Security Appliance Access
   viii. Practice Questions - Section 6.5

f. **Demilitarized Zones (DMZ)**
   i. Demilitarized Zones (9:49)
   ii. Configuring a DMZ (5:42)
   iii. Configure a DMZ
   iv. DMZ Facts
   v. Practice Questions - Section 6.6

g. **Firewalls**
   i. Firewalls (5:33)
   ii. Firewall Facts
   iii. Configuring a Perimeter Firewall (9:47)
   iv. Configure a Perimeter Firewall
   v. Practice Questions - Section 6.7

h. **Network Address Translation (NAT)**
   i. Network Address Translation (15:57)
   ii. Configuring NAT (5:11)
   iii. NAT Facts
   iv. Practice Questions - Section 6.8

i. **Virtual Private Networks (VPN)**
   i. Virtual Private Networks (VPNs) (10:16)
   ii. Configuring a VPN (4:25)

iii. Configure a Remote Access VPN
iv. Configure a VPN Connection iPad
v. VPN Facts
vi. VPN Protocol Facts
vii. Practice Questions - Section 6.9

j. **Web Threat Protection**
   i. Web Threat Protection (9:29)
   ii. Configuring Web Threat Protection (4:26)
   iii. Configure Web Threat Protection
   iv. Web Threat Protection Facts
   v. Practice Questions - Section 6.10

k. **Network Access Control (NAC)**
   i. Network Access Protection (19:58)
   ii. Implementing NAP with DHCP Enforcement (15:56)
   iii. NAP Facts
   iv. Practice Questions - Section 6.11

l. **Wireless Overview**
   i. Wireless Networking Overview (5:35)
   ii. Wireless Antenna Types (8:03)
   iii. Wireless Networking Facts
   iv. Wireless Encryption (6:46)
   v. Wireless Encryption Facts
   vi. Configuring a Wireless Connection (12:22)
   vii. Secure a Wireless Network
   viii. Practice Questions - Section 6.12

m. **Wireless Attacks**
   i. Wireless Attacks (13:29)
   ii. Wireless Attack Facts
   iii. Using Wireless Attack Tools (9:06)
   iv. Detecting Rogue Hosts (7:37)
   v. Practice Questions - Section 6.13

n. **Wireless Defenses**
   i. Wireless Security Considerations (12:54)
   ii. Wireless Authentication (4:40)
   iii. Wireless Authentication Facts
   iv. Configuring a Wireless Access Point (19:54)
   v. Obscure a Wireless Network
   vi. Configure a Wireless Profile
   vii. Configuring a Captive Portal (12:02)
   viii. Wireless Security Facts
   ix. Practice Questions - Section 6.14

VII. NETWORK DEFENSES

a. **Network Devices**
   i. Network Devices (5:51)
   ii. Network Device Facts
   iii. Practice Questions - Section 7.1

b. **Network Device Vulnerabilities**
   i. Device Vulnerabilities (1:47)
   ii. Device Vulnerability Facts
   iii. Searching Defaultpasswords.com (1:23)
   iv. Securing a Switch (3:21)
   v. Secure a Switch
   vi. Practice Questions - Section 7.2

c. **Switch Attacks**
   i. Switch Attacks (5:04)
   ii. Switch Attack Facts
   iii. Practice Questions - Section 7.3

d. **Router Security**
   i. Router Security (8:57)
   ii. Router Security Facts
   iii. Practice Questions - Section 7.4

e. **Switch Security**
   i. Switch Security (13:01)
   ii. Switch Loop Protection (10:47)
   iii. Switch Security Facts
   iv. Configuring VLANs from the CLI (4:32)
   v. Explore VLANs from the CLI
   vi. Configuring VLANs (3:32)
   vii. Explore VLANs
   viii. Hardening a Switch (14:10)
   ix. Harden a Switch
   x. Secure Access to a Switch
   xi. Secure Access to a Switch 2
   xii. Practice Questions - Section 7.5

f. **Intrusion Detection and Prevention**
   i. Intrusion Detection (7:14)
   ii. Detection vs. Prevention Controls (7:50)
   iii. IDS Facts
   iv. Implementing Intrusion Monitoring (3:33)
   v. Implementing Intrusion Prevention (7:51)
   vi. Implement Intrusion Prevention
   vii. Practice Questions - Section 7.6

g. **SAN Security**
   i. SAN Security Issues (14:32)
   ii. Configuring an iSCSI SAN (9:57)
   iii. SAN Security Facts
   iv. Practice Questions - Section 7.7

VIII. **HOST DEFENSES**

a. **Malware**
   i. Malware (9:28)
   ii. Malware Facts

iii. Malware Protection Facts
iv. Implementing Malware Protections (23:43)
v. Using Windows Defender (14:22)
vi. Configure Windows Defender
vii. Practice Questions - Section 8.1

b. **Password Attacks**
   i. Password Attacks (2:04)
   ii. Password Attack Facts
   iii. Using Rainbow Tables (4:48)
   iv. Capturing Passwords (5:40)
   v. Practice Questions - Section 8.2

c. **Windows System Hardening**
   i. Operating System Hardening (5:13)
   ii. Hardening Facts
   iii. Hardening an Operating System (6:41)
   iv. Managing Automatic Updates (18:31)
   v. Configure Automatic Updates
   vi. Configuring Windows Firewall (10:11)
   vii. Configure Windows Firewall
   viii. Configuring Windows Firewall Advanced Features (16:59)
   ix. Configuring Parental Controls (18:21)
   x. Configure Parental Controls
   xi. Practice Questions - Section 8.3

d. **Hardening Enforcement**
   i. Hardening Enforcement with GPOs (1:50)
   ii. Using Security Templates and Group Policy (6:53)
   iii. Configuring GPOs to Enforce Security (15:24)
   iv. Hardening Enforcement Facts
   v. Manage Services with Group Policy
   vi. Practice Questions - Section 8.4

e. **File Server Security**

i. File Server Security (7:58)
ii. Scanning for Open Ports (3:52)
iii. File System Security Facts
iv. File Permission Facts
v. Configuring NTFS Permissions (14:05)
vi. Configure NTFS Permissions
vii. Disable Inheritance
viii. Practice Questions - Section 8.5

f. **Linux Host Security**
   i. Linux Host Security (7:10)
   ii. Removing Unneeded Services and Scanning Ports (6:30)
   iii. Network Security Facts
   iv. Practice Questions - Section 8.6

g. **Static Environment Security**
   i. Security Risks in Static Environments (4:26)
   ii. Static Environment Security Facts
   iii. Practice Questions - Section 8.7

IX. APPLICATION DEFENSES

a. **Web Application Attacks**
   i. Web Application Attacks (2:49)
   ii. Cross-site Request Forgery (XSRF) Attack (10:51)
   iii. Injection Attacks (14:30)
   iv. Header Manipulation (9:01)
   v. Zero Day Application Attacks (6:59)
   vi. Client Side Attacks (6:22)
   vii. Web Application Attack Facts
   viii. Preventing Cross-site Scripting (4:05)
   ix. Practice Questions - Section 9.1

b. **Internet Browsers**
   i. Managing Security Zones and Add-ons (20:26)

ii. Configuring IE Enhanced Security (9:11)
iii. Managing Cookies (12:38)
iv. Configure Cookie Handling
v. Clearing the Browser Cache (9:28)
vi. Clear the Browser Cache
vii. Implementing Popup Blockers (7:26)
viii. Configure IE Popup Blocker
ix. Internet Explorer Security Facts
x. Enforcing IE Settings through GPO (12:47)
xi. Enforce IE Settings through GPO
xii. Configure IE Preferences in a GPO
xiii. Practice Questions - Section 9.2

c. **E-mail**
   i. E-mail Security (4:43)
   ii. E-mail Security Facts
   iii. Protecting a Client from Spam (10:29)
   iv. Securing an E-mail Server (2:45)
   v. Configure E-mail Filters
   vi. Securing E-mail on iPad (5:52)
   vii. Secure E-mail on iPad
   viii. Practice Questions - Section 9.3

d. **Network Applications**
   i. Network Application Security (2:19)
   ii. Spim (3:43)
   iii. Using Peer-to-peer Software (3:04)
   iv. Securing Windows Messenger (2:48)
   v. Configuring Application Control Software (9:05)
   vi. Network Application Facts
   vii. Practice Questions - Section 9.4

e. **Virtualization**
   i. Virtualization Introduction (4:01)

ii. Virtualization Benefits (3:08)
iii. Load Balancing with Virtualization (10:40)
iv. Creating Virtual Machines (4:22)
v. Managing Virtual Machines (5:09)
vi. Create Virtual Machines
vii. Adding Virtual Network Adapters (1:30)
viii. Creating Virtual Switches (3:26)
ix. Create Virtual Switches
x. Virtualization Facts
xi. Practice Questions - Section 9.5

f. **Application Development**

i. Secure Coding Concepts (16:18)
ii. Application Hardening (11:02)
iii. Application Development Security Facts
iv. Hardening Applications on Linux (4:26)
v. Implementing Application Whitelisting with AppLocker (13:03)
vi. Implement Application Whitelisting with AppLocker
vii. Implementing Data Execution Preventions (DEP) (4:01)
viii. Implement Data Execution Preventions (DEP)
ix. Hardening Applications Facts
x. NoSQL Security (5:18)
xi. NoSQL Security Facts
xii. Practice Questions - Section 9.6

X. **DATA DEFENSES**

a. **Redundancy**

i. Redundancy (4:55)
ii. Redundancy Measurement Parameters (5:12)
iii. Redundancy Facts
iv. RAID (7:27)
v. Implementing RAID (6:16)
vi. RAID Facts

vii. Configure Fault Tolerant Volumes
viii. Clustering (9:06)
ix. Clustering Facts
x. Practice Questions - Section 10.1

b. **Backup and Restore**
   i. Backup and Restore (13:27)
   ii. Backup and Restore Facts
   iii. Backup Management Facts
   iv. Backing Up Workstations (6:18)
   v. Back Up a Workstation
   vi. Restoring Workstation Data from Backup (2:19)
   vii. Back Up a Domain Controller
   viii. Restoring Server Data from Backup (2:12)
   ix. Practice Questions - Section 10.2

c. **File Encryption**
   i. Encrypting File System (EFS) (11:47)
   ii. Securing Files using EFS (11:45)
   iii. Encrypt Files with EFS
   iv. PGP and GPG (4:34)
   v. Encrypting Files with GPG (4:58)
   vi. BitLocker and Database Encryption (13:02)
   vii. Configuring BitLocker (6:17)
   viii. Configure BitLocker with a TPM
   ix. File Encryption Facts
   x. Practice Questions - Section 10.3

d. **Secure Protocols**
   i. Secure Protocols (8:44)
   ii. Secure Protocols 2 (15:26)
   iii. Secure Protocols Facts
   iv. Adding SSL to a Web Site (5:23)
   v. Allow SSL Connections

vi. IPSec (5:14)
vii. IPSec Facts
viii. Requiring IPSec for Communications (14:22)
ix. Practice Questions - Section 10.4

e. **Cloud Computing**

i. Cloud Computing Introduction (15:59)
ii. Cloud Computing Security Issues (6:32)
iii. Cloud Computing Facts
iv. Practice Questions - Section 10.5

XI. ASSESSMENTS AND AUDITS

a. **Vulnerability Assessment**

i. Vulnerability Assessment (4:55)
ii. Vulnerability Assessment Facts
iii. Scanning a Network with Nessus (18:26)
iv. Scanning a Network with Retina (12:12)
v. Scanning for Vulnerabilities Using MBSA (6:02)
vi. Review a Vulnerability Scan 1
vii. Review a Vulnerability Scan 2
viii. Review a Vulnerability Scan 3
ix. Performing Port and Ping Scans (2:36)
x. Checking for Weak Passwords (9:21)
xi. Practice Questions - Section 11.1

b. **Penetration Testing**

i. Penetration Testing (2:32)
ii. Penetration Testing Facts
iii. Exploring Penetration Testing Tools (11:22)
iv. Practice Questions - Section 11.2

c. **Protocol Analyzers**

i. Protocol Analyzers (3:07)
ii. Protocol Analyzer Facts

iii. Analyzing Network Traffic (6:50)
iv. Practice Questions - Section 11.3

d. **Log Management**
   i. Logs (3:25)
   ii. Log Facts
   iii. Logging Events with Event Viewer (3:52)
   iv. Windows Event Subscriptions (10:36)
   v. Configuring Source-initiated Subscriptions (4:50)
   vi. Configuring Remote Logging on Linux (8:23)
   vii. Remote Logging Facts
   viii. Practice Questions - Section 11.4

e. **Audits**
   i. Audits (3:13)
   ii. Audit Facts
   iii. Auditing the Windows Security Log (11:41)
   iv. Configure Advanced Audit Policy
   v. Auditing Device Logs (6:57)
   vi. Enable Device Logs
   vii. Practice Questions - Section 11.5

CURSO DE SEGURIDAD INFORMÁTICA

TI

POLÍTICAS DE PAGO

• Precios en **Pesos Mexicanos** - Excepto casos que se indique en otra moneda de manera expresa
• **LIQUIDACIÓN TOTAL** – Aplica previa al inicio del evento
• **DESCUENTO POR PRONTO PAGO** - Aplica liquidando el total de la inversión hasta 5 días hábiles previos al evento
• **POLÍTICAS DE PRECIOS Y DESCUENTOS** - Sujetas a términos y condiciones de IMECAF
• **FINANCIAMIENTO** – NO aplica

MÉTODOS DE PAGO

TARJETA DE CRÉDITO / DÉBITO
• VISA y MASTER CARD - No requiere presentación física
• AMERICAN EXPRESS - Si no es por PayPal, requiere presentación física
MESES SIN INTERESES
•3, 6, 9 Y 12 MSI – Tarjetas Banamex
•PayPal (Según las opciones disponibles en la plataforma)
TRANSFERENCIA INTERBANCARIA
• BANAMEX - Clabe 002180414600184021
DEPÓSITO BANCARIO
• BANAMEX - Cuenta 18402
• Sucursal 4146
TRANSFERENCIA O DEPÓSITO REQUIERE REFERENCIA
• Colocar cualquiera de los siguientes datos como referencia:
• Nombre, razón social, RFC o número de factura
BENEFICIARIO
• IMECAF México, SC

IMECAF®

Arquímedes 130
Dpcho. 205
Col. Polanco,
CDMX 11570

TEL. **55 1085 1515**
800 236 0800
info@imecaf.com

www.imecaf.com

CURSO DE SEGURIDAD INFORMÁTICA

TI

POLÍTICAS DE CONFIRMACIÓN Y CANCELACIÓN

PENALIZACIONES
NO APLICA - Notificando hasta 6 días hábiles previos al evento
• **20%** - Notificando con menos de 6 días hábiles previos al evento - Se podrá elegir otro Curso pagando la diferencia. En caso de reincidencia, aplica penalización del **100%**
• **100%** - NO SHOW (No Asistencia) o notificando con menos de 72 hrs. hábiles previas al evento
• **CANCELACIONES CON TARJETA DE CRÉDITO / DÉBITO** - Se les descontarán las comisiones efectuadas por el banco emisor (incluyendo la opción de meses sin intereses, en su caso)

CONFIRMACIÓN OFICIAL

IMECAF notificará **5 días hábiles previos** al evento vía e-mail y/o teléfono del contacto proporcionado por la empresa contratante y ésta deberá confirmar por el mismo medio su asistencia.

Se sugiere realizar la gestión de **viáticos**, en su caso, una vez recibida | IMECAF no se hace responsable por gastos incurridos en este rubro.

IMECAF se reserva la posibilidad de cambios sin previo aviso por causas ajenas a su voluntad - Cursos sujetos a **QUÓRUM MÍNIMO**