

商学院校级硕士  
网络安全管理 MBA  
(CISO, 首席信息安全官)





## 商学院校级硕士 网络安全管理 MBA (CISO, 首席信息安全官)

- » 模式: 在线
- » 时长: 12个月
- » 学位: TECH 科技大学
- » 课程表: 自由安排时间
- » 考试模式: 在线

网页链接: [www.techtitute.com/cn/school-of-business/professional-master-degree/master-mba-cybersecurity-management-ciso-chief-information-security-officer](http://www.techtitute.com/cn/school-of-business/professional-master-degree/master-mba-cybersecurity-management-ciso-chief-information-security-officer)

# 目录

01 欢迎	02 为什么在TECH学习?	03 为什么选择我们的课程?	04 目标
4	6	10	14
	05 能力	06 结构和内容	07 方法
	20	26	46
	08 我们学生的特质	09 课程管理	10 对你事业的影响
	54	58	82
		11 对你公司的好处	12 学位
		86	90

# 01 欢迎

今天的社会是超级连接的。信息时代允许公民在点击一个按钮时了解任何数据。但这也意味着，虚拟威胁是当今时代的主流，使公司比以往任何时候都更有可能成为恶意软件的接收方，这些恶意软件会破坏公司的生产和安全，甚至暴露客户和员工的个人数据，并暴露其IT弱点。虽然这一领域的保护是IT专家的工作，但越来越多的首席收入官和其他管理人员选择专门从事这一领域的工作，试图阻止网络犯罪分子，避免成为他们攻击的目标。出于这个原因，TECH创建了这个课程，在这个课程中，商业专业人士将通过一个易于学生理解的教学大纲找到当前最相关的信息。因此，凭借所获得的知识，毕业生将能够成功担任首席信息安全官，这一职位正逐渐升温并拥有广阔的增长前景。



网络安全管理 MBA (CISO, 首席信息安全官)  
TECH 科技大学





“

通过国际知名专家授课的10节大师班，  
提升您在网络安全管理方面的技能”

02

# 为什么在TECH学习?

TECH是世界上最大的100%在线商业学校。它是一所精英商学院，具有最大的学术需求模式。一个国际高绩效和管理技能强化培训的中心。



“

TECH是一所站在技术前沿的大学, 它将所有资源交给学生支配, 以帮助他们取得商业成功”

## TECH 科技大学



### 创新

该大学提供一种在线学习模式,将最新的教育科技与最大的教学严谨性相结合。一种具有最高国际认可度的独特方法,将为学生提供在不断变化的世界中发展的钥匙,在这个世界上,创新必须是所有企业家的基本承诺。

“由于在节目中加入了创新的互动式多视频系统,被评为“微软欧洲成功案例”。



### 最高要求

TECH的录取标准不是经济方面的。在这所大学学习没有必要进行大量投资。然而,为了从TECH毕业,学生的智力和能力的极限将受到考验。该机构的学术标准非常高。

**95%** | TECH学院的学生成功完成学业



### 联网

来自世界各地的专业人员参加TECH,因此,学生将能够建立一个庞大的联系网络,对他们的未来很有帮助。

**+100,000**

每年培训的管理人员

**+200**

不同国籍的人



### 赋权

学生将与最好的公司和具有巨大声望和影响力的专业人士携手成长。TECH已经与7大洲的主要经济参与者建立了战略联盟和宝贵的联系网络。

**+500**

| 与最佳公司的合作协议



### 人才

该计划是一个独特的建议,旨在发挥学生在商业领域的才能。这是一个机会,你可以利用它来表达你的关切和商业愿景。

TECH帮助学生在这个课程结束后向世界展示他们的才华。



### 多文化背景

通过在TECH学习,学生将享受到独特的体验。你将在一个多文化背景下学习。在一个具有全球视野的项目中,由于该项目,你将能够了解世界不同地区的工作方式,收集最适合你的商业理念的创新信息。

TECH的学生来自200多个国家。

TECH追求卓越,为此,有一系列的特点,使其成为一所独特的大学:



### 分析报告

TECH探索学生批判性的一面,他们质疑事物的能力,他们解决问题的能力和他们的人际交往能力。



### 优秀的学术成果

TECH为学生提供最好的在线学习方法。大学将再学习方法(国际公认的研究生学习方法)与哈佛大学商学院的案例研究相结合。传统和前卫在一个艰难的平衡中,在最苛刻的学术行程中。



### 规模经济

TECH是世界上最大的网上大学。它拥有超过10,000个大学研究生课程的组合。而在新经济中,数量+技术=颠覆性价格。这确保了学习费用不像在其他大学那样昂贵。



### 向最好的人学习

TECH教学团队在课堂上解释了导致他们在其公司取得成功的原因,在一个真实、活泼和动态的环境中工作。全力以赴提供优质专业的教师,使学生在事业上有所发展,在商业世界中脱颖而出。

来自20个不同国籍的教师。



在TECH,你将有机会接触到学术界最严格和最新的案例研究"



03

# 为什么选择我们的课程？

完成科技课程意味着在高级商业管理领域取得职业成功的可能性倍增。

这是一个需要努力和奉献的挑战，但它为我们打开了通往美好未来的大门。学生将从最好的教学团队和最灵活、最创新的教育方法中学习。





“

我们拥有最著名的教师队伍和市场上最完整的教学大纲,这使我们能够为您提供最高学术水平的培训”

该方案将提供众多的就业和个人利益,包括以下内容。

01

### 对学生的职业生涯给予明确的推动

通过在TECH学习,学生将能够掌握自己的未来,并充分开发自己的潜力。完成该课程后,你将获得必要的技能,在短期内对你的职业生涯作出积极的改变。

本专业70%的学员在不到2年的时间内实现了职业的积极转变。

02

### 制定公司的战略和全球愿景

TECH提供了一般管理的深刻视野,以了解每个决定如何影响公司的不同职能领域。

我们对公司的全球视野将提高你的战略眼光。

03

### 巩固高级商业管理的学生

在TECH学习,为学生打开了一扇通往非常重要的专业全景的大门,使他们能够将自己定位为高级管理人员,对国际环境有一个广阔的视野。

你将在100多个高层管理的真实案例中工作。

04

### 承担新的责任

在该课程中,将介绍最新的趋势、进展和战略,以便学生能够在不断变化的环境中开展专业工作。

45%的参训人员在内部得到晋升。

05

### 进入一个强大的联系网络

TECH将其学生联系起来,以最大限度地增加机会。有同样关注和渴望成长的学生。你将能够分享合作伙伴、客户或供应商。

你会发现一个对你的职业发展至关重要的联系网络。

06

### 以严格的方式开发公司项目

学生将获得深刻的战略眼光,这将有助于他们在考虑到公司不同领域的情况下开发自己的项目。

我们20%的学生发展自己的商业理念。

07

### 提高软技能和管理技能

TECH帮助学生应用和发展他们所获得的知识,并提高他们的人际交往能力,使他们成为有所作为的领导者。

提高你的沟通和领导能力,为你的职业注入活力。

08

### 成为一个独特社区的一部分

学生将成为由精英经理人、大公司、著名机构和来自世界上最著名大学的合格教授组成的社区的一部分:TECH 科技大学社区。

我们给你机会与国际知名的教授团队一起进行专业学习。

# 04 目标

这个 TECH 的课程旨在加强企业管理人员的专业技能,他们除了在自己的行动领域高度专业化之外,还将在这个课程中找到一个独特的机会,在一个非常重要的部门中得到提高,因为他们将学习如何预防可能对企业造成严重损害的互联网威胁。通过这种方式,他们将成为不同分支的专业专家,因此他们将能够控制公司的所有领域,从而成为首席信息安全官。





“

由于TECH提供的优越培训, 增加你的培训, 实现你的工作目标, 有了这个课程”

TECH 会把学生的目标作为自己的，  
并与学生一同致力达成

网络安全管理 MBA (CISO, 首席信息安全官) 将培养学生具备以下能力:

01

分析分析师在网络安全的作用

02

深入研究社会工程学及方法

03

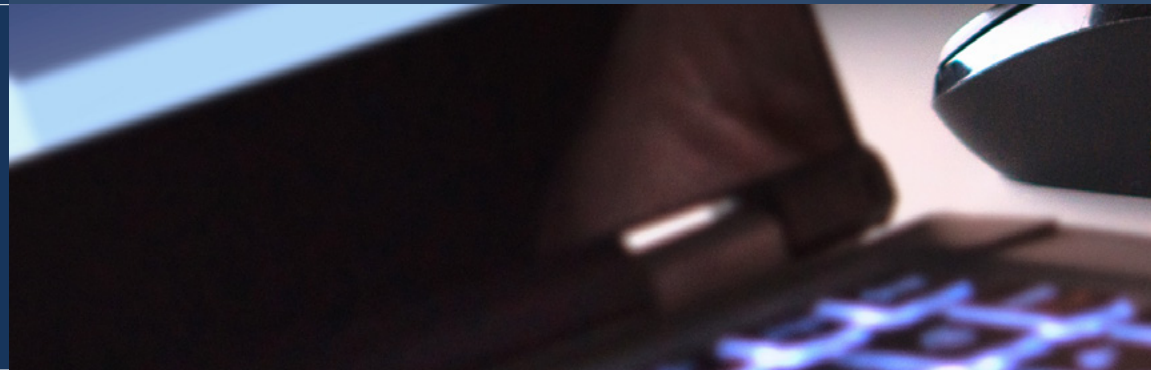
检查 OSINT、HUMINT、OWASP、PTEC、OSSTM 和  
OWISAM 方法

04

执行风险分析并了解风险指标

05

确定正确使用匿名性和使用 TOR、I2P 和 Freenet 等网络



06

学习专业知识以执行安全审计

08

考察最重要的威胁检测和预防系统

09

评估新的威胁检测系统, 以及它们相对于更传统解决方案的演变

07

制定适当的使用政策

10

分析当前主要的移动平台、特点和用途



11

识别、分析和评估物联网项目各部分的安全风险

12

评估获得的信息并制定预防和黑客攻击机制

13

将逆向工程应用于网络安全环境

14

完成对开发的软件进行的测试

15

收集所有现有证据和数据以进行法证报告



16

正确提交法证报告

18

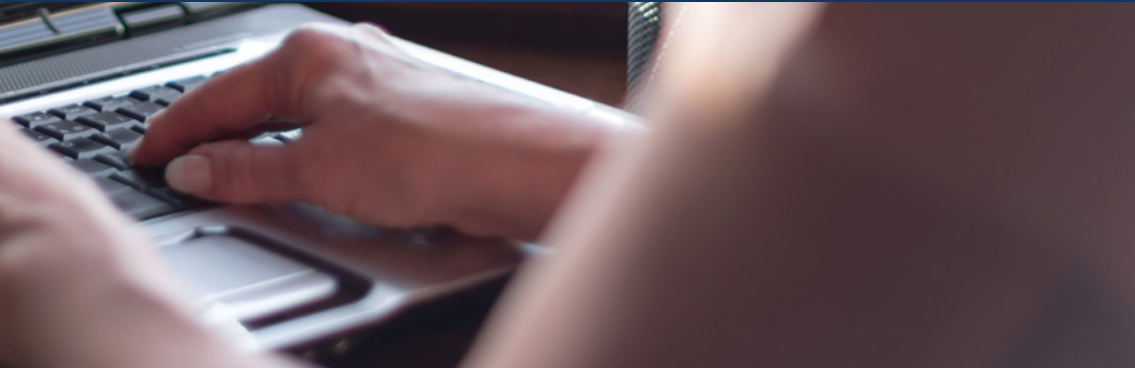
检查新兴技术的风险

19

汇编与计算机安全相关的不同技术

17

分析计算机安全的当前和未来情况





# 05 能力

这个网络安全管理 MBA (CISO, 首席信息安全官) 是为了提高商业领域专业人士的竞争力。因此, 在学习结束时, 学生将获得必要的能力, 在最创新的教学方法基础上发展高质量和最新的实践。毫无疑问, 这一方案将改善他们的培训, 使他们在日常实践中更有竞争力, 统一管理人员必须了解和实施的IT安全的所有相关方面。





“

进入计算机安全的研究, 提高你的技能, 控制潜在的网络威胁”

01

了解网络安全的使用方法

02

评估每种类型的威胁, 并在每种情况下提供最佳解决方案

03

发展完整的智能解决方案以在事件发生时进行自动化行为

04

了解如何评估与公司内外漏洞相关的风险



05

了解物联网随着时间推移的演变和影响

06

证明系统易受攻击, 出于预防目的对其进行攻击并解决上述问题

07

在不同的环境中应用沙盒技术

08

了解优秀开发人员必须遵循的准则以遵守必要的安全性





09

开展防御性安全行动

10

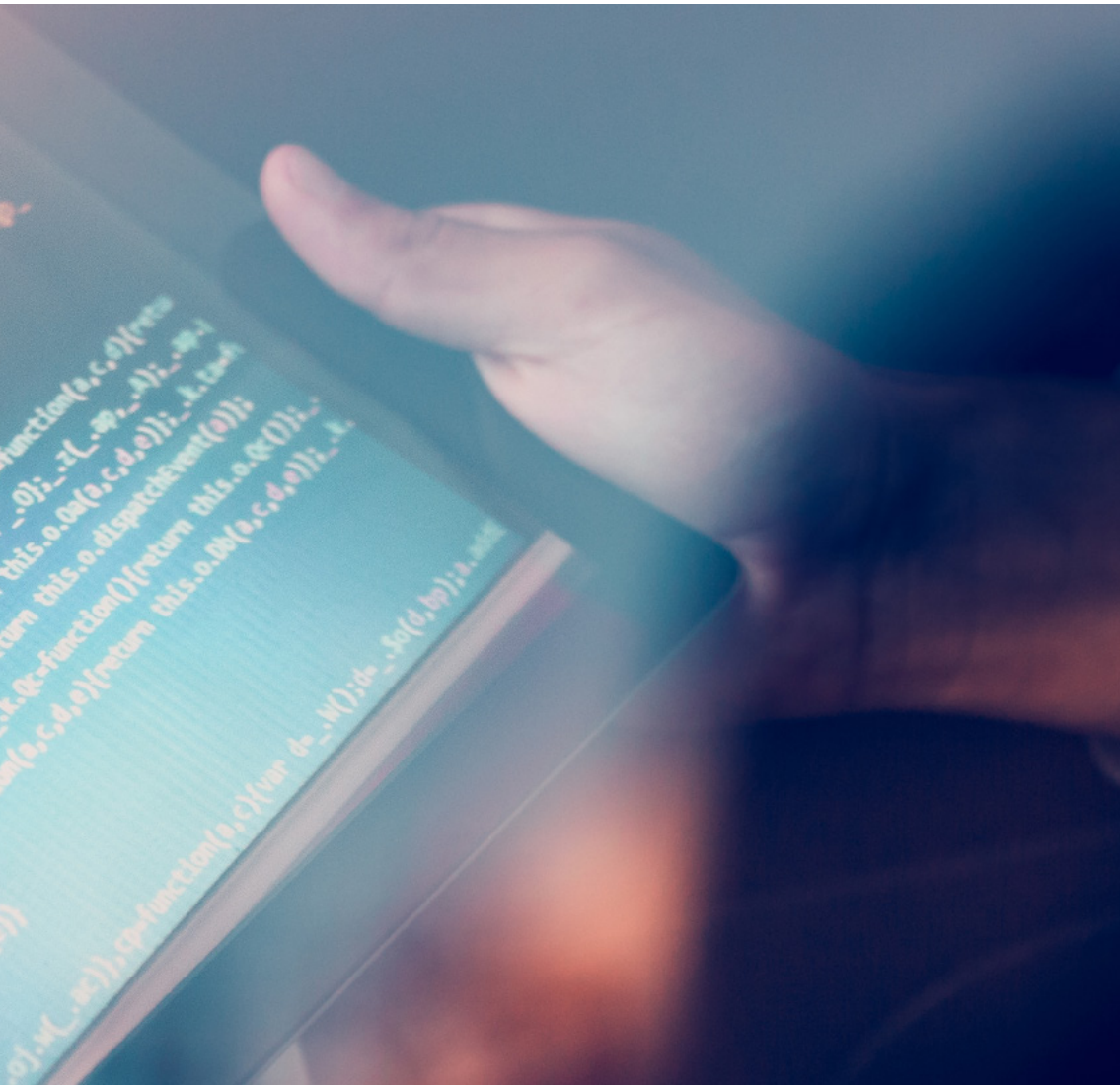
对计算机安全有深刻而专业的认识

11

了解如何为智能手机和便携式设备应用安全流程







12

了解进行所谓的道德黑客 攻击并保护公司免受网络攻击的方法

13

能够调查网络安全事件

14

区分现有的攻击和防御技术

# 06

## 结构和内容

这个TECH课程的设计是为了满足那些希望拓宽IT安全知识的商业专业人士的专业需求，这是一个基础的领域，以便能够控制可能对公司构成巨大风险的潜在威胁。通过这种方式，MBA将帮助他们获得可以应用于实际工作的专业知识。为此，他们将使用一种完全在线的方法，使他们能够将学习与其他日常义务相结合。



“

这个方案对于检测贵公司可能的网络攻击至关重要”

## 教学大纲

TECH 科技大学的网络安全管理 MBA (CISO, 首席信息安全官) 课程是一个高强度的项目,旨在促进管理能力的发展,以便在不确定的环境中做出更为严格的决策。

在1500小时的学习过程中,学员将获得成功进行日常实践所需的技能。因此,它是一个真正的沉浸在真实的商业环境中。

这个课程深入处理商业的不同领域,旨在让管理人员从战略、国际和创新的角度理解教育管理。

一个为学生设计的计划,专注于你的专业提高,为他们在环境和能源管理领域取得优异成绩做准备。这是一个理解你和你公司需求的课程,通过基于最新趋势的创新内容,并得到最佳教育方法和卓越师资的支持。

此外,还包括10节独特的大师班,作为教学材料的一部分,处于技术和教育的前沿。这些课程由国际知名的情报、网络安全和颠覆性技术专家设计,是专业人士在网络安全管理领域获得专长和有效管理公司相关部门的重要资源。

这个课程需要12个月,分为15个模块:

模块1	网络情报与网络安全
模块2	主机的安全
模块3	网络安全(周边)
模块4	智能手机的安全
模块5	物联网安全
模块6	道德黑客
模块7	逆向工程
模块8	安全发展
模块9	取证分析
模块10	计算机安全现在和未来的挑战
模块11	公司的领导力、道德和社会责任
模块12	人事和人才管理
模块13	经济-财务管理
模块14	商业管理与战略营销
模块15	执行管理



### 何时,何地,如何授课?

TECH你提供了完全在网上开发这一方案的可能性。在培训持续的12个月中,你可以学生将能够访问这个课程的所有内容,这将使你能够自我管理你的学习时间。

这将是一个独特而关键的教育旅程,将成为你专业发展的决定性一步,助你实现明显的飞跃。

## 模块 1. 网络情报与网络安全

### 1.1. 网络情报

- 1.1.1. 网络情报
  - 1.1.1.1. 智能
    - 1.1.1.1.1. 情报周期
  - 1.1.1.2. 网络情报
  - 1.1.1.3. 网络情报与网络安全
- 1.1.2. 情报分析员
  - 1.1.2.1. 情报分析师的角色
  - 1.1.2.2. 情报分析员在评估活动中的偏见

### 1.2. 网络安全

- 1.2.1. 安全层
- 1.2.2. 识别网络威胁
  - 1.2.2.1. 外部威胁
  - 1.2.2.2. 内部威胁
- 1.2.3. 不利的行动
  - 1.2.3.1. 社会工程学
  - 1.2.3.2. 常用方法

### 1.3. 智能技术和工具

- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMINT
- 1.3.4. Linux 发行和工具
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

### 1.4. 评估方法

- 1.4.1. 情报分析
- 1.4.2. 组织获取信息的技术
- 1.4.3. 信息来源的可靠性和可信度
- 1.4.4. 分析方法
- 1.4.5. 情报结果展示

### 1.5. 审计和文件

- 1.5.1. IT安全审计
- 1.5.2. 审计文件和许可证
- 1.5.3. 审计的类型
- 1.5.4. 可交付的成果
  - 1.5.4.1. 技术报告
  - 1.5.4.2. 执行报告

### 1.6. 网络匿名

- 1.6.1. 使用匿名
- 1.6.2. 匿名技术 (Proxy, VPN)
- 1.6.3. TOR、Freenet 和 IP2 网络

### 1.7. 威胁和安全类型

- 1.7.1. 威胁类型
- 1.7.2. 实体安全
- 1.7.3. 网络安全
- 1.7.4. 逻辑安全
- 1.7.5. Web 应用程序的安全性
- 1.7.6. 移动设备的安全

### 1.8. 法规和合规性

- 1.8.1. RGPD
- 1.8.2. BORRAR
- 1.8.3. ISO 15000 系列
- 1.8.4. NIST 网络安全框架
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. 云法规
- 1.8.8. SOX
- 1.8.9. PCI

### 1.9. 风险分析和指标

- 1.9.1. 风险范围
- 1.9.2. 资产
- 1.9.3. 威胁
- 1.9.4. 漏洞
- 1.9.5. 风险评估
- 1.9.6. 风险处理

### 1.10. 网络安全领域的重要组织

- 1.10.1. 美国国家标准与技术研究院
- 1.10.2. 欧洲网络及信息安全局
- 1.10.3. 美洲国家组织
- 1.10.4. 南美国家联盟-南美进步论坛



**模块 2. 主机的安全****2.1. 后备副这个**

- 2.1.1. 备份策略
- 2.1.2. 适用于 Windows 的工具
- 2.1.3. Linux 的工具
- 2.1.4. macOS 的工具

**2.2. 用户的防毒软件**

- 2.2.1. 防毒软件的类型
- 2.2.2. 适用于 Windows 的防毒软件
- 2.2.3. linux 的防毒软件
- 2.2.4. MacOS的防毒软件
- 2.2.5. 智能手机的防毒软件

**2.3. 入侵探测器 - HIDS**

- 2.3.1. 入侵探测方法
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

**2.4. 这个地防火墙**

- 2.4.1. Windows 防火墙
- 2.4.2. Linux 的防火墙
- 2.4.3. MacOS 防火墙

**2.5. 密码管理器**

- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. 粘性密码
- 2.5.5. RoboForm

**2.6. 网络钓鱼检测器**

- 2.6.1. 手动钓鱼检测器
- 2.6.2. 网络钓鱼工具

**2.7. 间谍软件**

- 2.7.1. 回避机制
- 2.7.2. 反间谍软件工具

**2.8. 追踪器**

- 2.8.1. 系统保护措施
- 2.8.2. 反追踪工具

**2.9. EDR-端点检测和响应**

- 2.9.1. EDR 系统行为
- 2.9.2. EDR 和防病毒软件的区别
- 2.9.3. EDR系统的未来

**2.10. 控制安装软件**

- 2.10.1. 存储库和软件商店
- 2.10.2. 允许或禁止的软件列表
- 2.10.3. 更新标准
- 2.10.4. 安装软件的权限



### 模块 3. 网络安全(周边)

#### 3.1. 威胁检测和预防系统

- 3.1.1. 安全事件的总体框架
- 3.1.2. 目前的防御系统: 纵深防御和 SOC
- 3.1.3. 当前的网络架构
- 3.1.4. 用于检测和预防事故的工具类型
  - 3.1.4.1. 基于网络的系统
  - 3.1.4.2. 基于主机的系统
  - 3.1.4.3. 集中式系统
- 3.1.5. 阶段/主机、容器和无服务器的通信和检测

#### 3.2. 防火墙

- 3.2.1. 防火墙的类型
- 3.2.2. 攻击和缓解
- 3.2.3. Linux 内核的常用防火墙 防火墙
  - 3.2.3.1. UFW
  - 3.2.3.2. Nftables 和 iptables
  - 3.2.3.3. 防火墙(Firewalld)
- 3.2.4. 基于系统日志的检测系统
  - 3.2.4.1. TCP 包装器
  - 3.2.4.2. BlockHosts 和 DenyHosts
  - 3.2.4.3. Fai2ban

#### 3.3. 入侵检测和预防系统 (IDS/IPS)

- 3.3.1. 对 IDS/IPS 的攻击
- 3.3.2. IDS/IPS 系统
  - 3.3.2.1. Snort
  - 3.3.2.2. Suricata

#### 3.4. 下一代防火墙(NGFW)

- 3.4.1. NGFW与传统防火墙的区别
- 3.4.2. 核心能力
- 3.4.3. 商务解决方案
- 3.4.4. cloud防火墙
  - 3.4.4.1. 云 VPC 架构
  - 3.4.4.2. 云ACLs
  - 3.4.4.3. 安全组

#### 3.5. 代理服务器

- 3.5.1. proxy类型
- 3.5.2. proxy使用代理优缺点

#### 3.6. 防毒引擎

- 3.6.1. 恶意软件和IOC的总体背景
- 3.6.2. 防毒引擎的问题

#### 3.7. 邮件保护系统

- 3.7.1. 反垃圾邮件
  - 3.7.1.1. 黑白名单
  - 3.7.1.2. 贝叶斯过滤器
- 3.7.2. 邮件网关(MGW)

#### 3.8. SIEM

- 3.8.1. 组件和架构
- 3.8.2. 关联规则和用例
- 3.8.3. SIEM 系统的当前挑战

#### 3.9. SOAR

- 3.9.1. SOAR 和 SIEM: 敌人或盟友
- 3.9.2. SOAR系统的未来

#### 3.10. 其他基于网络的系统

- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. 蜜罐 和 蜜网
- 3.10.4. CASB

**模块 4. 智能手机的安全****4.1. 移动设备的世界**

- 4.1.1. 移动平台类型
- 4.1.2. 设备
- 4.1.3. 安卓设备

**4.2. 移动安全管理**

- 4.2.1. OWASP 移动安全项目
  - 4.2.1.1. 十大漏洞
- 4.2.2. 通信、网络 and 连接模式

**4.3. 商业环境的移动设备**

- 4.3.1. 风险
- 4.3.2. 设备监控
- 4.3.3. 移动设备管理 (MDM)

**4.4. 用户隐私和数据安全**

- 4.4.1. 信息状态
- 4.4.2. 安全数据存储
  - 4.4.2.1. iOS 的安全存储
  - 4.4.2.2. 安卓的安全存储
- 4.4.3. 应用程序开发中的正确做法

**4.5. 漏洞和攻击媒介**

- 4.5.1. 漏洞
- 4.5.2. 攻击向量
  - 4.5.2.1. 恶意软件
  - 4.5.2.2. 泄露数据
  - 4.5.2.3. 操作数据

**4.6. 主要威胁**

- 4.6.1. 用户未强制
- 4.6.2. 恶意软件
  - 4.6.2.1. 恶意软件的类型
- 4.6.3. 社会工程学
- 4.6.4. 数据泄露
- 4.6.5. 信息盗窃
- 4.6.6. 不安全的 Wi-Fi 网络
- 4.6.7. 过时的软件
- 4.6.8. 恶意应用程序
- 4.6.9. 弱密码
- 4.6.10. 安全设置薄弱或不存在
- 4.6.11. 物理访问
- 4.6.12. 丢失或被盗的设备
- 4.6.13. 身份冒充 (诚信)
- 4.6.14. 弱或损坏的密码学
- 4.6.15. 拒绝服务 (DoS)

**4.7. 主要攻击**

- 4.7.1. 网络钓鱼攻击
- 4.7.2. 与通信模式相关的攻击
- 4.7.3. smishing 攻击
- 4.7.4. 加密劫持攻击
- 4.7.5. 中间人攻击

**4.8. 黑客攻击**

- 4.8.1. Rooting 和 Jailbreaking
- 4.8.2. 移动攻击剖析
  - 4.8.2.1. 威胁传播
  - 4.8.2.2. 在设备上安装恶意软件
  - 4.8.2.3. 持久性
  - 4.8.2.4. 有效载荷执行和信息提取
- 4.8.3. 入侵 iOS 设备: 机制和工具
- 4.8.4. 入侵 Android 设备: 机制和工具

**4.9. 渗透测试**

- 4.9.1. iOS 渗透测试
- 4.9.2. 安卓 渗透测试
- 4.9.3. 工具

**4.10. 保护和安全**

- 4.10.1. 安全设定
  - 4.10.1.1. iOS 设备
  - 4.10.1.2. 安卓设备
- 4.10.2. 安防措施
- 4.10.3. 保护工具

## 模块 5. 物联网安全

### 5.1. 设备

- 5.1.1. 设备类型
- 5.1.2. 标准化架构
  - 5.1.2.1. ONEM2M
  - 5.1.2.2. IoTWF
- 5.1.3. 应用协议
- 5.1.4. 连接技术

### 5.2. 物联网设备。应用领域

- 5.2.1. 智能家居
- 5.2.2. 智慧城市
- 5.2.3. 运输
- 5.2.4. 可穿戴设备
- 5.2.5. 健康领域
- 5.2.6. IIoT

### 5.3. 通讯协议

- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

### 5.4. 智能家居

- 5.4.1. 家庭自动化
- 5.4.2. 网络
- 5.4.3. 家用电器
- 5.4.4. 警惕和安全

### 5.5. 智慧城市

- 5.5.1. 照明
- 5.5.2. 气象
- 5.5.3. 安全

### 5.6. 运输

- 5.6.1. 地点
- 5.6.2. 付款和获得服务
- 5.6.3. 连接性

### 5.7. 可穿戴设备

- 5.7.1. 智能衣服
- 5.7.2. 智能首饰
- 5.7.3. 智能手表

### 5.8. 健康领域

- 5.8.1. 运动/心率监测
- 5.8.2. 监测患者和老年人
- 5.8.3. 可植入的
- 5.8.4. 手术机器人

### 5.9. 连接性

- 5.9.1. WiFi/网关
- 5.9.2. 蓝牙
- 5.9.3. 内置连接

### 5.10. 证券化

- 5.10.1. 专用网络
- 5.10.2. 密码管理器
- 5.10.3. 使用加密协议
- 5.10.4. 使用提示

**模块 6. 道德黑客****6.1. 工作环境**

- 6.1.1. Linux 发行版
  - 6.1.1.1. Kali Linux - 进攻性安全
  - 6.1.1.2. 鸚鵡系统
  - 6.1.1.3. Ubuntu
- 6.1.2. 虚拟化系统
- 6.1.3. 沙盒
- 6.1.4. 实验室部署

**6.2. 方法**

- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. 美国国家标准与技术研究院
- 6.2.4. PTES
- 6.2.5. ISSAF

**6.3. Footprinting**

- 6.3.1. 开源情报 (OSINT)
- 6.3.2. 搜索数据泄露和漏洞
- 6.3.3. 使用被动工具

**6.4. 网络扫描**

- 6.4.1. 扫描工具
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. 其他扫描工具
- 6.4.2. 扫描技术
- 6.4.3. 防火墙和IDS规避技术
- 6.4.4. 标志提取
- 6.4.5. 网络图

**6.5. 枚举**

- 6.5.1. SMTP 枚举
- 6.5.2. DNS 枚举
- 6.5.3. NetBIOS 和 Samba 枚举
- 6.5.4. LDAP 枚举
- 6.5.5. SNMP 枚举
- 6.5.6. 其他枚举技术

**6.6. 漏洞扫描**

- 6.6.1. 漏洞分析解决方案
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. 漏洞评分系统
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

**6.7. 无线网络攻击**

- 6.7.1. 无线网络黑客攻击方法
  - 6.7.1.1. 发现Wi-Fi
  - 6.7.1.2. 流量分析
  - 6.7.1.3. aircrack攻击
    - 6.7.1.3.1. WEP攻击
    - 6.7.1.3.2. WPA/WPA2攻击
  - 6.7.1.4. 孪生恶魔攻击
  - 6.7.1.5. WPS攻击
  - 6.7.1.6. 干扰
- 6.7.2. 无线安全工具

**6.8. 入侵网络服务器**

- 6.8.1. 跨站脚这个攻击
- 6.8.2. CSRF
- 6.8.3. 会话Hijacking
- 6.8.4. SQL注入攻击

**6.9. 利用漏洞**

- 6.9.1. 使用已知漏洞
- 6.9.2. 使用metasploit
- 6.9.3. 使用恶意软件
  - 6.9.3.1. 定义和范围
  - 6.9.3.2. 生成恶意软件
  - 6.9.3.3. 绕过防病毒解决方案

**6.10. 持久性**

- 6.10.1. Rootkit 的安装
- 6.10.2. ncat 的使用
- 6.10.3. 为后门使用 计划任务
- 6.10.4. 用户创建
- 6.10.5. HIDS 检测

## 模块 7. 逆向工程

### 7.1. 编译器

- 7.1.1. 代码类型
- 7.1.2. 编译器的阶段
- 7.1.3. 符号表
- 7.1.4. 错误的处理程序
- 7.1.5. GCC 编译器

### 7.2. 编译器中的解析类型

- 7.2.1. 词法分析
  - 7.2.1.1. 术语
  - 7.2.1.2. 词汇成分
  - 7.2.1.3. LEX 词法分析器
- 7.2.2. 句法分析
  - 7.2.2.1. 文法无上下文
  - 7.2.2.2. 解析类型
    - 7.2.2.2.1. 自上向下分析
    - 7.2.2.2.2. 自下而上分析
  - 7.2.2.3. 语法树和派生
  - 7.2.2.4. 解析器的类型
    - 7.2.2.4.1. LR (从左到右) 解析器
    - 7.2.2.4.2. LALR 解析器
- 7.2.3. 语义分析
  - 7.2.3.1. 文法的属性
  - 7.2.3.2. S-属性
  - 7.2.3.3. L-属性

### 7.3. 汇编器数据结构

- 7.3.1. 变数
- 7.3.2. 数组
- 7.3.3. 指引
- 7.3.4. 结构
- 7.3.5. 物品

### 7.4. 汇编代码结构

- 7.4.1. 选择结构
  - 7.4.1.1. 如果, 否则 如果, 否则
  - 7.4.1.2. 转变
- 7.4.2. 迭代结构
  - 7.4.2.1. For
  - 7.4.2.2. While
  - 7.4.2.3. 休息时间的使用
- 7.4.3. 职能

### 7.5. x86硬件架构

- 7.5.1. x86 处理器架构
- 7.5.2. x86 数据结构
- 7.5.3. x86 代码结构

### 7.6. ARM硬件架构

- 7.6.1. ARM 处理器架构
- 7.6.2. ARM 数据结构
- 7.6.3. ARM 代码结构

### 7.7. 静态代码分析

- 7.7.1. 反汇编程序
- 7.7.2. IDA
- 7.7.3. 代码重建器

### 7.8. 动态代码分析

- 7.8.1. 行为分析
  - 7.8.1.1. 工业电子通讯
  - 7.8.1.2. 监测
- 7.8.2. Linux 代码调试器
- 7.8.3. Windows 的代码调试器

### 7.9. 沙盒

- 7.9.1. 沙盒的架构
- 7.9.2. 避免 沙箱
- 7.9.3. 检测技术
- 7.9.4. 躲避技巧
- 7.9.5. 反措施
- 7.9.6. Linux中的沙盒
- 7.9.7. Windows中的沙盒
- 7.9.8. MacOS中的沙盒
- 7.9.9. Android中的沙盒

### 7.10. 恶意软件分析

- 7.10.1. 恶意软件分析方法
- 7.10.2. 恶意软件混淆技术
  - 7.10.2.1. 可执行的混淆
  - 7.10.2.2. 执行环境的限制
- 7.10.3. 恶意软件分析工具

**模块 8. 安全发展****8.1. 安全发展**

- 8.1.1. 质量、功能和安全
- 8.1.2. 保密性、完整性和可用性
- 8.1.3. 软件开发生命周期

**8.2. 需求阶段**

- 8.2.1. 认证控制
- 8.2.2. 控制角色和权限
- 8.2.3. 风险导向的要求
- 8.2.4. 特权批准

**8.3. 分析和设计阶段**

- 8.3.1. 访问组件和系统管理
- 8.3.2. 审计追踪
- 8.3.3. 会话管理
- 8.3.4. 历史数据
- 8.3.5. 正确的错误处理
- 8.3.6. 职责分开

**8.4. 实施和编码阶段**

- 8.4.1. 保护开发环境
- 8.4.2. 准备技术文件
- 8.4.3. 安全加密
- 8.4.4. 通讯安全

**8.5. 安全编码最佳实践**

- 8.5.1. 输入数据验证
- 8.5.2. 输出数据编码
- 8.5.3. 编程风格
- 8.5.4. 变更日志管理
- 8.5.5. 密码实践
- 8.5.6. 错误和日志管理
- 8.5.7. 文件管理
- 8.5.8. 内存管理
- 8.5.9. 安全功能的标准化和重用

**8.6. 服务器准备和加固**

- 8.6.1. 管理服务器上的用户、组别和角色
- 8.6.2. 软件安装
- 8.6.3. 服务器加固
- 8.6.4. 应用环境的配置

**8.7. DB准备和硬化**

- 8.7.1. 优化数据库引擎优化
- 8.7.2. 为应用程序创建自己的用户
- 8.7.3. 为用户分配精确的权限
- 8.7.4. 数据库加固加固

**8.8. 测试阶段**

- 8.8.1. 质安全控制的质量控制
- 8.8.2. 阶段性代码检查
- 8.8.3. 配置管理验证
- 8.8.4. 黑盒测试

**8.9. 准备向生产过渡**

- 8.9.1. 执行变更控制
- 8.9.2. 执行分步生产程序
- 8.9.3. 执行回滚过程
- 8.9.4. 预生产阶段的测试

**8.10. 维护阶段**

- 8.10.1. 基于风险的保险
- 8.10.2. 白盒安全维护测试
- 8.10.3. 黑盒安全维护测试

## 模块 9. 取证分析

### 9.1. 数据采集和复制

- 9.1.1. 易失性数据采集
  - 9.1.1.1. 系统信息
  - 9.1.1.2. 网络信息
  - 9.1.1.3. 波动率定律
- 9.1.2. 静态数据采集
  - 9.1.2.1. 创建重复图像
  - 9.1.2.2. 为监管链准备文件
- 9.1.3. 获取数据的验证方法
  - 9.1.3.1. 适用于Linux的方法
  - 9.1.3.2. 适用于Windows的方法

### 9.2. 反取证技术的评估和失败

- 9.2.1. 反法医技术的目标
- 9.2.2. 删除数据
  - 9.2.2.1. 删除数据和文件
  - 9.2.2.2. 恢复文件
  - 9.2.2.3. 恢复已删除的分区
- 9.2.3. 密码保护
- 9.2.4. 隐写术
- 9.2.5. 安全删除设备
- 9.2.6. 加密

### 9.3. 操作系统的取证分析

- 9.3.1. Windows 取证
- 9.3.2. Linux 取证
- 9.3.3. Mac 取证

### 9.4. 网络取证

- 9.4.1. 日志分析
- 9.4.2. 数据相关
- 9.4.3. 网络研究
- 9.4.4. 网络取证要遵循的步骤

### 9.5. 网络取证

- 9.5.1. 网络攻击调查
- 9.5.2. 攻击检测
- 9.5.3. IP 地址的位置

### 9.6. 数据库取证

- 9.6.1. MSSQL取证分析
- 9.6.2. MySQL取证分析
- 9.6.3. PostgreSQL取证分析
- 9.6.4. MongoDB取证分析

### 9.7. 云取证分析

- 9.7.1. 云的犯罪类型
  - 9.7.1.1. 以云为主体
  - 9.7.1.2. 云作为对象
  - 9.7.1.3. 云作为工具
- 9.7.2. 云取证的挑战
- 9.7.3. 云存储服务调查
- 9.7.4. 云取证工具

### 9.8. 电子邮件犯罪调查

- 9.8.1. 邮件系统
  - 9.8.1.1. 邮件客户端
  - 9.8.1.2. 邮件服务器
  - 9.8.1.3. SMTP 服务器
  - 9.8.1.4. POP3 服务器
  - 9.8.1.5. IMAP4 服务器
- 9.8.2. 邮件犯罪
- 9.8.3. 邮件信息
  - 9.8.3.1. 标准标题
  - 9.8.3.2. 扩展标题
- 9.8.4. 调查这些罪行的步骤
- 9.8.5. 电子邮件取证工具

### 9.9. 移动取证

- 9.9.1. 手机网络
  - 9.9.1.1. 网络类型
  - 9.9.1.2. CDR内容
- 9.9.2. 用户识别模块 (SIM)
- 9.9.3. 逻辑获取
- 9.9.4. 物理获取
- 9.9.5. 文件系统获取

### 9.10. 起草和提交法证报告

- 9.10.1. 取证报告的重要方面
- 9.10.2. 报告的分类和类型
- 9.10.3. 撰写报告指南
- 9.10.4. 提交报告
  - 9.10.4.1. 作证前的准备
  - 9.10.4.2. 证人陈述
  - 9.10.4.3. 与媒体打交道



**模块 10. 计算机安全现在和未来的挑战****10.1. 区块链技术**

- 10.1.1. 应用的领域
- 10.1.2. 保密保证
- 10.1.3. 不可抵赖的保证

**10.2. 数字货币**

- 10.2.1. Bitcoins
- 10.2.2. 加密货币
- 10.2.3. 加密货币挖矿
- 10.2.4. 金字塔计划
- 10.2.5. 其他潜在的犯罪和问题

**10.3. Deepfake**

- 10.3.1. 媒体的影响
- 10.3.2. 对社会的危害
- 10.3.3. 检测机制

**10.4. 人工智能的未来**

- 10.4.1. 人工智能和认知计算
- 10.4.2. 用于简化客户服务

**10.5. 数字隐私**

- 10.5.1. 网络数据的价值
- 10.5.2. 网络数据的使用
- 10.5.3. 隐私和数字身份管理

**10.6. 网络冲突、网络罪犯和网络攻击**

- 10.6.1. 网络安全对国际冲突的影响
- 10.6.2. 网络攻击对普通人群的影响
- 10.6.3. 网络犯罪分子的类型保护措施

**10.7. 远程办公**

- 10.7.1. Covid19 期间和之后的远程办公革命
- 10.7.2. 访问瓶颈
- 10.7.3. 攻击面的变化
- 10.7.4. 工人的需要

**10.8. 新兴无线技术**

- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. 毫米波
- 10.8.4. “变得聪明”而不是“获得更多”的趋势

**10.9. 网络的未来寻址**

- 10.9.1. IP寻址的当前问题
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. IPv4+ 相对于IPv4的优势
- 10.9.5. IPv6 相对于IPv4的优势

**10.10. 提高民众早期和持续培训意识的挑战**

- 10.10.1. 当前的政府策
- 10.10.2. 民众对学习的抵制
- 10.10.3. 公司将采用的培训计划

## 模块 11. 公司的领导力、道德和社会责任

### 11.1. 全球化与治理

- 11.1.1. 治理和公司治理
- 11.1.2. 企业公司治理的基本原则
- 11.1.3. 董事会在公司治理框架中的角色

### 11.2. 领导力

- 11.2.1. 领导力。一个概念性的方法
- 11.2.2. 公司领导力
- 11.2.3. 领导者在企业管理中的重要性

### 11.3. 跨文化管理

- 11.3.1. 跨文化管理的概念
- 11.3.2. 对民族文化知识的贡献
- 11.3.3. 多元化管理

### 11.4. 管理发展和领导力

- 11.4.1. 管理发展的概念
- 11.4.2. 领导力的概念
- 11.4.3. 领导力理论
- 11.4.4. 领导风格
- 11.4.5. 领导力中的情报
- 11.4.6. 今天的领导力挑战

### 11.5. 可持续发展

- 11.5.1. 可持续性和可持续发展
- 11.5.2. 2030 年议程
- 11.5.3. 可持续发展的公司

### 11.6. 企业社会责任

- 11.6.1. 企业社会责任的国际维度
- 11.6.2. 履行企业社会责任
- 11.6.3. 公司社会责任的影响及衡量

### 11.7. 负责任管理的系统和工具

- 11.7.1. RSC: 企业社会责任
- 11.7.2. 实施负责任管理战略的基本要素
- 11.7.3. 实施企业社会责任管理系统的步骤
- 11.7.4. CSR工具和标准

### 11.8. 跨国公司与人权

- 11.8.1. 全球化、跨国企业和人权
- 11.8.2. 跨国公司面临国际法
- 11.8.3. 跨国公司有关人权的法律文书

### 11.9. 法律环境和公司治理

- 11.9.1. 国际进口和出口规则
- 11.9.2. 知识产权和工业产权
- 11.9.3. 国际劳工法

**模块 12. 人事和人才管理****12.1. 战略人员管理**

- 12.1.1. 战略管理和人力资源
- 12.1.2. 人员管理战略

**12.2. 基于能力的人力资源管理**

- 12.2.1. 潜力分析
- 12.2.2. 薪酬政策
- 12.2.3. 职业/继任计划

**12.3. 绩效评估和绩效管理**

- 12.3.1. 绩效管理
- 12.3.2. 绩效管理:目标和过程

**12.4. 人才和人员管理的创新**

- 12.4.1. 战略人才管理模式
- 12.4.2. 人才的识别、培训和发展
- 12.4.3. 忠诚度和保留率
- 12.4.4. 积极主动,勇于创新

**12.5. 激励**

- 12.5.1. 激励的这个质
- 12.5.2. 期望理论
- 12.5.3. 需求理论
- 12.5.4. 激励和经济补偿

**12.6. 培养高绩效团队**

- 12.6.1. 高绩效团队;自我管理团队
- 12.6.2. 高绩效自我管理团队的管理方法

**12.7. 更换管理层**

- 12.7.1. 更换管理层
- 12.7.2. 变更管理流程的类型
- 12.7.3. 变革管理的阶段或阶段

**12.8. 谈判和冲突管理**

- 12.8.1. 谈判
- 12.8.2. 冲突管理
- 12.8.3. 危机管理

**12.9. 沟通管理**

- 12.9.1. 企业内外沟通
- 12.9.2. 通讯部门
- 12.9.3. 公司的传媒负责人Dircom 简介

**12.10. 人才的生产力、吸引、留存和激活**

- 12.10.1. 生产力
- 12.10.2. 吸引和保留人才的杠杆

模块 13. 经济-财务管理

13.1. 经济环境

- 13.1.1. 宏观经济环境和国家金融体系
- 13.1.2. 金融机构
- 13.1.3. 金融市场
- 13.1.4. 金融资产
- 13.1.5. 金融部门的其他实体

13.2. 管理会计

- 13.2.1. 基这个概念
- 13.2.2. 公司资产
- 13.2.3. 公司负债
- 13.2.4. 公司净资产
- 13.2.5. 损益表

13.3. 信息系统和商业智能

- 13.3.1. 基这个原理和分类
- 13.3.2. 成这个分配阶段和方法
- 13.3.3. 成这个中心的选择和影响

13.4. 预算和管理控制

- 13.4.1. 预算模型
- 13.4.2. 资本预算
- 13.4.3. 运营预算
- 13.4.4. 财政部预算
- 13.4.5. 预算跟踪

13.5. 财务管理

- 13.5.1. 公司的财务决策
- 13.5.2. 财务部
- 13.5.3. 现金盈余
- 13.5.4. 与财务管理相关的风险
- 13.5.5. 财务管理 风险管理

13.6. 金融规划

- 13.6.1. 财务规划的定义
- 13.6.2. 财务规划中要采取的行动
- 13.6.3. 创建和制定企业战略
- 13.6.4. 现金流量表
- 13.6.5. 当前表

13.7. 企业财务战略

- 13.7.1. 企业战略和融资来源
- 13.7.2. 企业融资的金融产品

13.8. 战略融资

- 13.8.1. 自筹资金
- 13.8.2. 自有资金增加
- 13.8.3. 混合资源
- 13.8.4. 通过中介机构融资

13.9. 金融分析和规划

- 13.9.1. 资产负债表分析
- 13.9.2. 损益表分析
- 13.9.3. 盈利能力分析

13.10. 案例/问题的分析和解决

- 13.10.1. 设计与纺织工业股份公司的财务信息 (INDITEX)

**模块 14. 商业管理与战略营销****14.1. 商业管理**

- 14.1.1. 商业管理的概念框架
- 14.1.2. 业务战略和规划
- 14.1.3. 商业总监的角色

**14.2. 营销**

- 14.2.1. 营销的概念
- 14.2.2. 营销的基本要素
- 14.2.3. 公司的营销活动

**14.3. 战略营销管理**

- 14.3.1. 战略营销理念
- 14.3.2. 战略营销规划的概念
- 14.3.3. 战略营销规划过程的各个阶段

**14.4. 数字和电子商务营销**

- 14.4.1. 数字营销和电子商务的目标
- 14.4.2. 数字营销和媒体使用
- 14.4.3. 电子商务。一般背景
- 14.4.4. 电商类目
- 14.4.5. 电子商务的优点和缺点 与传统商业相比

**14.5. 数字营销以加强品牌**

- 14.5.1. 提高品牌声誉的在线策略
- 14.5.2. 品牌内容和讲故事

**14.6. 吸引和信任客户的数字营销**

- 14.6.1. 通过互联网的忠诚度和参与战略
- 14.6.2. 客户关系管理
- 14.6.3. 分区过大

**14.7. 数字运动管理**

- 14.7.1. 什么是数字广告活动?
- 14.7.2. 启动在线营销活动的步骤
- 14.7.3. 数字广告活动中的错误

**14.8. 销售策略**

- 14.8.1. 销售策略
- 14.8.2. 销售方式

**14.9. 企业沟通**

- 14.9.1. 概念
- 14.9.2. 组织沟通的重要性
- 14.9.3. 组织中的沟通类型
- 14.9.4. 组织中沟通的功能
- 14.9.5. 沟通的要素
- 14.9.6. 沟通问题
- 14.9.7. 通讯场景

**14.10. 沟通和数字声誉**

- 14.10.1. 在线声誉
- 14.10.2. 如何衡量数字声誉?
- 14.10.3. 在线声誉工具
- 14.10.4. 在线声誉报告
- 14.10.5. 品牌 在线的

## 模块 15. 执行管理

### 15.1. 一般管理

- 15.1.1. 一般管理概念
- 15.1.2. 总经理的行动
- 15.1.3. 总干事和他的职能
- 15.1.4. 管理局工作的转型

### 15.2. 经理和他或她的职能。组织文化及其方法

- 15.2.1. 经理和他或她的职能。组织文化及其方法

### 15.3. 业务管理

- 15.3.1. 领导力的重要性
- 15.3.2. 价值链
- 15.3.3. 质量管理

### 15.4. 公众演讲和发言人培训

- 15.4.1. 人际沟通
- 15.4.2. 沟通技巧和影响力
- 15.4.3. 沟通障碍

### 15.5. 个人和组织沟通的工具

- 15.5.1. 人际交往
- 15.5.2. 人际交往的工具
- 15.5.3. 组织内的沟通
- 15.5.4. 组织中的工具

### 15.6. 危机情况下的沟通

- 15.6.1. 危机
- 15.6.2. 危机的各个阶段
- 15.6.3. 信息：内容和时刻

### 15.7. 准备一个危机计划

- 15.7.1. 对潜在问题的分析
- 15.7.2. 教学
- 15.7.3. 工作人员是否充足

### 15.8. 情绪智力

- 15.8.1. 情绪智力和沟通
- 15.8.2. 自信、同理心和积极倾听
- 15.8.3. 自尊与情感沟通

### 15.9. 个人品牌

- 15.9.1. 发展个人品牌的策略
- 15.9.2. 个人品牌建设的法则
- 15.9.3. 建立个人品牌的工具

### 15.10. 领导力和团队管理

- 15.10.1. 领导力和领导风格
- 15.10.2. 领导者的能力和挑战
- 15.10.3. 变更流程管理
- 15.10.4. 多元文化团队管理



“

这个课程将为我们打开通往新的职业世界的大门”



# 07 方法

这个培训计划提供了一种不同的学习方式。我们的方法是通过循环的学习模式发展起来的: **Re-learning**。

这个教学系统被世界上一些最著名的医学院所采用,并被**新英格兰医学杂志**等权威出版物认为是最有效的教学系统之一。





“

发现 Re-learning, 这个系统放弃了传统的线性学习, 带你体验循环教学系统: 这种学习方式已经证明了其巨大的有效性, 尤其是在需要记忆的科目中”



## TECH商学院使用案例研究来确定所有内容的背景

我们的方案提供了一种革命性的技能和知识发展方法。我们的目标是在一个不断变化, 竞争激烈和高要求的环境中加强能力建设。

“

和TECH,你可以体验到一种正在动摇  
世界各地传统大学基础的学习方式”



该课程使你准备好在不确定的环境中  
面对商业挑战, 使你的企业获得成功。



我们的课程使你准备好在不确定的环境中面对新的挑战,并取得事业上的成功。

## 一种创新并不同的学习方法

该技术课程是一个密集的培训课程,从头开始创建,为国内和国际最高水平的管理人员提供挑战和商业决策。由于这种方法,个人和职业成长得到了促进,向成功迈出了决定性的一步。案例法是构成这一内容的基础的技术,确保遵循最新的经济,社会和商业现实。



你将通过合作活动和真实案例,学习如何解决真实商业环境中的复杂情况”

在世界顶级商学院存在的时间里,案例法一直是最广泛使用的学习系统。1912年开发的案例法是为了让法律学生不仅在理论内容的基础上学习法律,案例法向他们展示真实的复杂情况,让他们就如何解决这些问题作出明智的决定和价值判断。1924年,它被确立为哈佛大学的一种标准教学方法。

在特定情况下,专业人士应该怎么做?这就是我们在案例法中面临的问题,这是一种以行动为导向的学习方法。在整个课程中,学生将面对多个真实案例。他们必须整合所有的知识,研究,论证和捍卫他们的想法和决定。

## Re-learning 方法

TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合, 在每节课中结合了个不同的教学元素。

我们用最好的100%在线教学方法加强案例研究: Re-learning。

我们的在线系统将允许你组织你的时间和学习节奏, 使其适应你的时间表。你将能够从任何有互联网连接的固定或移动设备上获取容。



在TECH, 你将用一种旨在培训未来管理人员的尖端方法进行学习。这种处于世界教育学前沿的方法被称为 Re-learning。

我们的商学院是唯一获准采用这种成功方法的西班牙语学校。2019年, 我们成功地提高了学生的整体满意度 (教学质量, 材料质量, 课程结构, 目标.....), 与西班牙语最佳在线大学的指标相匹配。



在我们的方案中,学习不是一个线性的过程,而是以螺旋式的方式发生(学习,解除学习,忘记和重新学习)。因此,我们将这些元素中的每一个都结合起来。这种方法已经培养了超过65万名大学毕业生,在生物化学,遗传学,外科,国际法,管理技能,体育科学,哲学,法律,工程,新闻,历史,金融市场和工具等不同领域取得了前所未有的成功。所有这些都是在一个高要求的环境中进行的,大学学生的社会经济状况很好,平均年龄为43.5岁。

Re-learning 将使你的学习事半功倍,表现更出色,使你更多地参与到训练中,培养批判精神,捍卫论点和对比意见:直接等同于成功。

从神经科学领域的最新科学证据来看,我们不仅知道如何组织信息,想法,图像y记忆,而且知道我们学到东西的地方和背景,这是我们记住它并将其储存在海马体的根本原因,并能将其保留在长期记忆中。

通过这种方式,在所谓的神经认知背景依赖的电子学习中,我们课程的不同元素与学员发展其专业实践的背景相联系。



该方案提供了最好的教育材料,为专业人士做了充分准备:



### 学习材料

所有的教学内容都是由教授该课程的专家专门为该课程创作的,因此,教学的发展是具体的。

然后,这些内容被应用于视听格式,创造了TECH在线工作方法。所有这些,都是用最新的技术,提供最高质量的材料,供学生使用。



### 大师课程

有科学证据表明第三方专家观察的有用性。

向专家学习可以加强知识和记忆,并为未来的困难决策建立信心。



### 管理技能实习

他们将在每个学科领域开展具体的管理能力发展活动。获得和培训高级管理人员在我们所处的全球化框架内所需的技能和能力的做法和新情况。

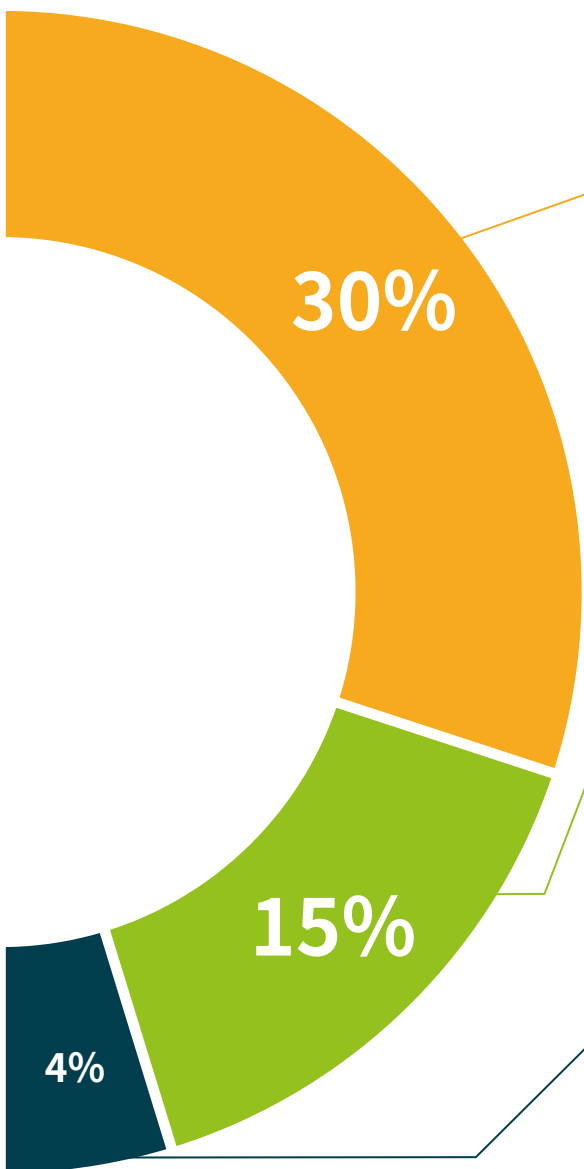


### 延伸阅读

最近的文章,共识文件和国际准则等。在TECH的虚拟图书馆里,学生可以获得他们完成培训所需的一切。







### 案例研究

他们将完成专门为这个学位选择的最佳案例研究。由国际上最好的高级管理专家介绍,分析和辅导的案例。



### 互动式总结

TECH团队以有吸引力和动态的方式将内容呈现在多媒体中,其中包括音频,视频,图像,图表和概念图,以强化知识。这个用于展示多媒体内容的独特教育系统被微软授予“欧洲成功案例”称号。



### 测试和循环测试

在整个课程中,通过评估和自我评估活动和练习,定期评估和重新评估学习者的知识:通过这种方式,学习者可以看到他/她是如何实现其目标的。



08

# 我们学生的特质

网络安全管理 MBA(首席信息安全官)课程是为那些希望通过优质教育提升专业能力的职业人士设计的。想在与商业相关的另一个分支,如IT,但更具体地说,IT安全方面拓宽知识的学生。一个针对有经验的专业人士的课程,他们相信更高的专业化是个人和专业改进的方法。





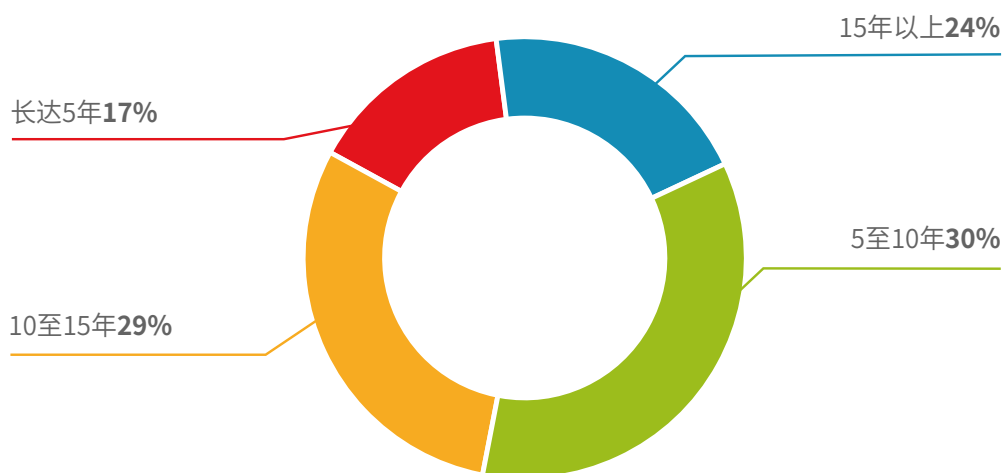
“

TECH的学生是具有丰富经验的专业人士,他们正在寻找一份更好的工作”

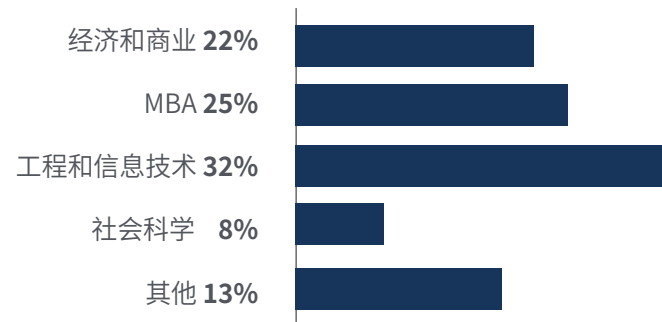
### 平均年龄

**35**岁至 **45**岁之间

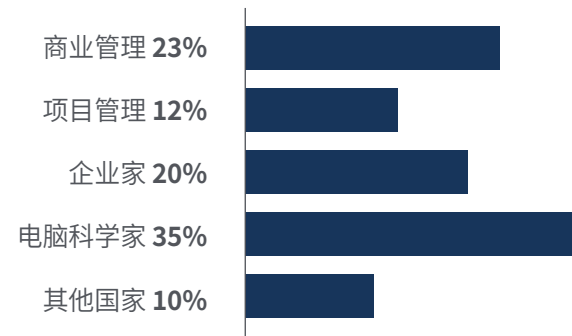
### 经验年限



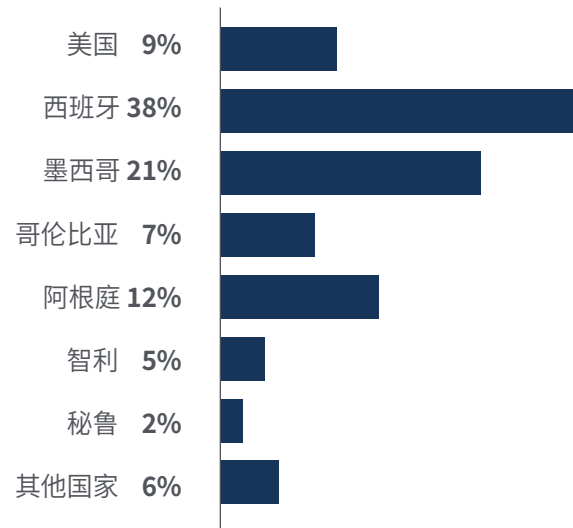
### 教育



### 学术概况



## 地域分布



## Jaime Díaz

首席收入官

"在我工作的商业环境中，我们处理大量的机密信息和相关数据，这些信息在错误的人手中，会给公司带来很大的问题。这就是为什么我有一段时间一直在考虑扩大我的网络安全知识，目的是自己控制所有可能对网络威胁最敏感的过程。感谢这个TECH方案，我已经能够提高我的技能，并在工作中变得更加自信"

# 09

## 课程管理

这个网络安全管理 MBA (CISO, 首席信息安全官) 是在这个领域具有丰富经验的专业人员, 包括专业和教育方面。他们在这一领域的专业性使他们拥有必要的资格, 为学生提供完整和高质量的学习科目, 这些科目对他们在商业世界的日常工作很有帮助。他们当然是相信高等教育是推动其专业发展和提高企业竞争力的途径的人。





“

经验丰富的教师, 帮助你在网络安全方面的专业性”



## 国际客座董事

Frederic Lemieux博士是国际公认的情报、国家安全、国土安全、网络安全和颠覆性技术领域的创新专家和灵感领袖。情报、国土安全、国土安全、网络安全和颠覆性技术。他在研究和教育方面的不懈努力和贡献，使他成为促进安全和了解当今新兴技术的关键人物。在他的职业生涯中，他曾在蒙特利尔大学、乔治-华盛顿大学和乔治城大学等多所知名院校构思和指导尖端学术课程。

在他的广泛背景中，他出版了许多重要著作，所有这些著作都与犯罪情报、警务、网络威胁和国际安全有关。刑事情报、警务、网络威胁和国际安全。他还在学术期刊上发表了大量文章，研究重大灾害期间的犯罪控制、反恐、情报机构和警务合作等问题，为网络安全领域做出了重大贡献。此外，他还各种国家和国际会议上担任小组成员和主旨发言人，在学术和专业领域树立了自己的典范。

莱米厄博士曾在各种学术、私人 and 政府组织中担任编辑和评估职务，这反映了他在其专业领域的影响力和追求卓越的决心。就这样，他享有盛誉的学术生涯使他成为了 MPS 项目的实践教授和教员主任。应用情报、网络安全风险管理、技术管理和信息技术管理，在乔治城大学。



## Lemieux, Frederic 博士

---

- 美国华盛顿州乔治敦网络安全风险管理硕士主任
- 乔治城大学技术管理硕士课程主任
- 乔治敦大学应用情报学硕士课程主任
- 乔治敦大学实习教授
- 他还获得了蒙特利尔大学犯罪学学院的犯罪学博士学位
- 拉瓦尔大学社会学硕士和心理学辅修学位
- 乔治城大学新课程圆桌委员会成员

“

感谢 TECH, 你将能够与世界上最优秀的专业人士一起学习”

## 国际客座董事

拥有超过20年全球人才招聘团队设计和领导经验的Jennifer Dove是招聘和技术战略方面的专家。在她的职业生涯中,她曾在多家财富50强企业的科技组织中担任高管职务,包括NBCUniversal和Comcast。她的职业历程使她在竞争激烈和高速增长的环境中脱颖而出。

作为Mastercard的全球人才招聘副总裁,她负责监督人才引进的策略和执行,与企业领导和人力资源负责人合作,以实现招聘的运营和战略目标。特别是,她的目标是创建多元化、包容性和高绩效的团队,以推动公司产品和服务的创新和增长。此外,她在吸引和留住全球顶尖人才的工具使用方面具有丰富经验。她还通过出版物、活动和社交媒体扩大Mastercard的雇主品牌和价值主张。

Jennifer Dove通过积极参与人力资源专业网络并为多家公司引进大量员工,展示了她对持续职业发展的承诺。在获得迈阿密大学组织传播学士学位后,她在各个领域的公司中担任了招聘管理职位。此外,她因在领导组织变革、将技术整合到招聘流程中以及开发应对未来挑战的领导力项目方面的能力而受到认可。她还成功实施了显著提高员工满意度和留任率的员工福利计划。



## Dove, Jennifer 女士

---

- Mastercard全球人才招聘副总裁, 纽约, 美国
- NBCUniversal Media 人才招聘总监, 纽约, 美国
- Comcast招聘负责人
- Rite Hire Advisory招聘总监
- Ardor NY Real Estate销售部执行副总裁
- Valerie August & Associates招聘总监
- BNC客户经理
- Vault客户经理
- 迈阿密大学组织传播学专业毕业

“

TECH 拥有一支卓越且专业的国际客座董事团队, 他们在全球市场中最前沿的公司中担任重要的领导角色”

## 国际客座董事

Rick Gauthier 是一位技术领导者, 在领先的跨国公司拥有数十年的工作经验。Rick Gauthier 在云服务和端到端流程改进领域有着突出的发展。他是公认的高效团队领导者和管理者, 在确保员工高度敬业方面展现出天赋。

他在战略和执行创新方面有着与生俱来的天赋, 善于开发新想法, 并以高质量的数据为其成功提供支持。他在 Amazon 的职业生涯使他能够管理和整合公司在美国的 IT 服务。在 Microsoft, 他领导着一支 104 人的团队, 负责提供全公司范围的 IT 基础设施, 并为整个公司的产品工程部门提供支持。

这些经验使他成为一名出色的管理者, 在提高效率、生产力和整体客户满意度方面能力出众。



## Gauthier, Rick 先生

---

- 美国西雅图 Amazon 公司区域 IT 经理
- Amazon 高级项目经理
- Wimmer Solutions 副总裁
- Microsoft 生产工程服务高级总监
- 西州长大学网络安全学位
- 潜水员技术学院颁发的商业潜水技术证书
- 常青州立学院环境研究学位

“

借此机会了解这个领域的最新发展,并将其应用到你的日常工作中”



## 国际客座董事

Romi Arman 是一位国际知名的专家,在数字化转型、营销、战略和咨询领域拥有超过二十年的经验。在他的广泛职业生涯中,他承担了各种风险,并始终是企业环境中创新和变革的倡导者。凭借这些专业知识,他与世界各地的首席执行官和企业组织合作,推动他们摒弃传统的商业模式。因此,他帮助像壳牌这样的公司成为以客户为中心和数字化的市场领导者。

Arman设计的战略具有显著的影响,因为这些战略使多家公司改善了消费者、员工和股东的体验。这位专家的成功可以通过诸如客户满意度(CSAT)、员工参与度和每家公司的息税折旧摊销前利润(EBITDA)等可量化指标来衡量。

在他的职业生涯中,他还培养并领导了高绩效团队,这些团队甚至因其变革潜力而获得奖项。特别是在壳牌,Arman始终致力于克服三个挑战:满足客户复杂的脱碳需求,支持“有利可图的脱碳”,以及解决数据、数字和技术的碎片化问题。因此,他的努力证明了要实现可持续的成功,必须从消费者的需求出发,并为流程、数据、技术和文化的转型奠定基础。

此外,这位高管还以其对人工智能企业应用的精通而著称,他在伦敦商学院获得了相关的研究生学位。与此同时,他在物联网和Salesforce方面也积累了丰富的经验。





## Arman, Romi 先生

---

- 壳牌能源公司数字化转型总监 (CDO), 伦敦, 英国
- 壳牌能源公司全球电子商务与客户服务总监
- 壳牌在马来西亚吉隆坡的国家重点客户经理 (原始设备制造商和汽车零售商)
- 埃森哲高级管理顾问 (金融服务业), 新加坡
- 利兹大学毕业
- 伦敦商学院高管人工智能企业应用研究生
- 客户体验专业认证 (CCXP)
- IMD高管数字化转型课程

“

你想以最高质量的教育来更新你的知识吗?TECH为你提供最前沿的学术内容,由国际知名的专家设计”

## 国际客座董事

Manuel Arens 是一位经验丰富的数据管理专家，也是一支高素质团队的领导者。事实上，Arens 在谷歌的技术基础设施和数据中心部门担任全球采购经理一职，这是他职业生涯的大部分时间。这个公司总部位于加利福尼亚州山景城，为科技巨头的运营难题提供解决方案，如主数据完整性、供应商数据更新和供应商数据优先级。他领导了数据中心供应链规划和供应商风险评估，改进了流程和工作流程管理，从而大大节约了成本。

在为不同行业公司提供数字解决方案和领导力的十多年工作中，他在战略解决方案交付的各个方面，包括市场营销、媒体分析、测量和归因方面，都拥有丰富的经验。事实上，这个公司已因其工作获得了多个奖项，包括 BIM 领导奖、搜索领导奖、出口领导力生成计划奖和欧洲、中东和非洲地区最佳销售模式奖。

Arens 还担任过爱尔兰都柏林的销售经理。在担任这个职务期间，他在三年内将团队成员从 4 人增加到 14 人，并带领销售团队取得了丰硕成果，与团队成员以及跨职能团队进行了良好合作。他还曾在德国汉堡担任高级行业分析师，利用内部和第三方工具为 150 多家客户创建故事情节，为分析提供支持。编写和撰写深入报告，以展示对这个主题的掌握，包括对影响技术采用和传播的宏观经济和政治/监管因素的理解。

此外，他在 Eaton、Airbus 和 Siemens 等公司领导团队，积累了宝贵的客户管理和供应链管理经验。他特别擅长通过与客户建立有价值的关系并与组织各层级的人员（包括利益相关者、管理层、团队成员和客户）顺畅合作来不断超越期望。他的数据驱动方法和开发创新且可扩展解决方案的能力使他成为该领域的杰出领导者。



## Arens, Manuel 先生

---

- 谷歌全球采购经理, 美国山景城
- 美国谷歌 B2B 分析与技术高级经理
- 爱尔兰谷歌销售总监
- 德国谷歌高级工业分析师
- 爱尔兰谷歌客户经理
- 英国伊顿的应付账款
- 德国空中客车公司供应链经理

“

选择TECH吧!你将能够接触到最优质的教学材料、最前沿的技术和教育方法,这些都是由国际知名的专家实施的”

## 国际客座董事

Andrea La Sala 是一位经验丰富的市场营销高管, 他的项目对时尚领域产生了显著的影响。在其成功的职业生涯中, 他从事了与产品、商品销售和沟通相关的多项工作。这些都与诸如Giorgio Armani、Dolce&Gabbana、Calvin Klein等知名品牌紧密相关。

这位国际高端管理者的成果与他在将信息整合成清晰框架并执行与企业目标对齐的具体行动的能力密切相关。他以其主动性和适应快节奏工作的能力而闻名。此外, 这位专家还具有强烈的商业意识、市场洞察力和对产品的真正热情。

作为Giorgio Armani的全球品牌与商品销售总监, 他监督了多项针对服装和配饰的市场营销策略。其战术重点包括零售领域以及消费者需求和行为。在这一职位上, La Sala 还负责配置产品在不同市场的销售, 担任设计、沟通和销售部门的团队负责人。

此外, 在Calvin Klein或Gruppo Coin等公司, 他开展了推动结构、开发和销售不同系列的项目, 并负责制定有效的购买和销售活动日程。

他还管理了不同运营的条款、成本、流程和交货时间。

这些经历使Andrea La Sala 成为时尚和奢侈品领域的顶级和最具资格的企业领导者之一。他的卓越管理能力使他能够有效实施品牌的积极定位, 并重新定义其关键绩效指标 (KPI)。



## La Sala, Andrea 先生

---

- Giorgio Armani全球品牌与商品销售总监, Armani Exchange, 米兰, 意大利
- Calvin Klein商品销售总监
- Gruppo Coin品牌负责人
- Dolce&Gabbana品牌经理
- Sergio Tacchini S.p.A.品牌经理
- Fastweb市场分析师
- 皮埃蒙特东方大学商学与经济学专业毕业

“

TECH的国际顶级专家将为你提供一流的教学, 课程内容更新及时, 基于最新的科学证据。你还在等什么呢?立即报名吧"

## 国际客座董事

Mick Gram 是国际上在商业智能领域创新与卓越的代名词。他成功的职业生涯与在沃尔玛和红牛等跨国公司担任领导职位密切相关。这位专家以识别新兴技术的远见卓识而闻名，这些技术在长期内对企业环境产生了持久的影响。

此外，他被认为是数据可视化技术的先锋，这些技术将复杂的数据集简化，使其易于访问并促进决策过程。这一能力成为了他职业发展的基石，使他成为许多组织希望收集信息并基于这些信息制定具体行动的宝贵资产。

他最近几年最突出的项目之一是Walmart Data Cafe平台，这是全球最大的云端大数据分析平台。他还担任了红牛的商业智能总监，涵盖销售、分销、营销和供应链运营等领域。他的团队最近因在使用Walmart Luminate新API来获取买家和渠道洞察方面的持续创新而获得认可。

在教育背景方面，这位高管拥有多个硕士学位和研究生课程，曾在美国伯克利大学和丹麦哥本哈根大学等知名学府深造。通过持续的更新，专家获得了前沿的能力。因此，他被认为是新全球经济的天生领导者，专注于推动数据及其无限可能性。



## Gram, Mick 先生

---

- 红牛商业智能与分析总监, 洛杉矶, 美国
- Walmart Data Cafe商业智能解决方案架构师
- 独立商业智能与数据科学顾问
- Capgemini商业智能总监
- Nordea首席分析师
- SAS商业智能首席顾问
- UC Berkeley工程学院人工智能与机器学习高管教育
- 哥本哈根大学电子商务MBA高管课程
- 哥本哈根大学数学与统计学学士及硕士

“

在福布斯评选的世界上最好的在线大学学习”在这个MBA课程中, 你将获得访问由国际知名教师制作的丰富多媒体资源库”



## 国际客座董事

Scott Stevenson 是数字营销领域的杰出专家。他是数字营销专家，19 年来一直与娱乐业最强大的公司之一 华纳兄弟探索公司保持联系。在担任该职务期间，他在 监督包括社交媒体、搜索、展示和线性媒体在内的 各种数字平台 的物流和创意工作流程方面发挥了重要作用。

这位高管的领导力在推动付费媒体制作战略方面发挥了至关重要的作用，使其公司的转化率显著提高。这位高管在推动付费媒体制作战略方面发挥了至关重要的作用，从而显著 提高了 公司的转化率。与此同时，他还担任过其他职务，如原管理期间同一家跨国公司的营销服务总监和交通经理。

史蒂文森还参与了视频游戏的全球发行和 数字财产宣传活动。他还负责引入与 电视广告和预告片的 声音和图像内容的塑造、定稿和交付有关的运营战略。

此外，这位专家还拥有佛罗里达大学的电信学士学位和加利福尼亚大学的创意写作商院校级硕士，这充分证明了他在 沟通和讲故事方面的能力。此外，他还参加了哈佛大学职业发展学院关于 在商业中使用 人工智能的前沿课程。因此，他的专业履历是当前 市场营销和数字媒体领域最相关的履历之一。



## Stevenson, Scott 先生

---

- 华纳兄弟数字营销总监美国伯班克发现
- 华纳兄弟公司交通经理娱乐
- 加利福尼亚大学创意写作硕士
- 佛罗里达大学电信学士学位

“

与世界上最优秀的专家一起实现你的学术和职业目标!MBA 教师将指导您完成整个学习过程"

## 国际客座董事

Eric Nyquist 博士是国际体育领域的杰出专业人士，他的职业生涯令人瞩目，因其战略领导力以及在顶级体育组织中推动变革和创新的能力而闻名。

他曾担任多个高级职位，包括NASCAR的通讯与影响总监，总部位于美国佛罗里达州。在这一机构中积累了多年经验后，Nyquist博士还担任了多个领导职务，包括NASCAR战略发展高级副总裁和商务事务总监，负责管理从战略发展到娱乐营销等多个领域。

此外，Nyquist在芝加哥最重要的体育特许经营中留下了深刻印记。作为芝加哥公牛队和芝加哥白袜队的执行副总裁，他展示了在职业体育领域推动业务和战略成功的能力。

最后，值得一提的是，他的体育职业生涯始于纽约，担任Roger Goodell在国家橄榄球联盟(NFL)的首席战略分析师，并曾在美国足球联合会担任法律实习生。



## Nyquist, Eric 先生

---

- NASCAR通讯与影响总监, 佛罗里达, 美国
- NASCAR战略发展高级副总裁
- NASCAR战略规划副总裁
- NASCAR商务事务总监
- 芝加哥白袜队执行副总裁
- 芝加哥公牛队执行副总裁
- 国家橄榄球联盟(NFL)企业规划经理
- 美国足球联合会商务事务/法律实习生
- 芝加哥大学法学博士
- 芝加哥大学布斯商学院MBA
- Carleton College国际经济学学士

“

凭借这项100%在线的学士学位, 你将能够在不影响日常工作义务的情况下进行学习, 同时得到国际领域内顶级专家的指导。现在就报名!"

## 管理人员



### Fernández Sapena, Sonia 女士

- 马德里赫塔菲的国家计算机和电信参考中心的计算机安全和道德黑客培训师
- 认证的电子理事会讲师
- 获得以下认证的培训师: EXIN 道德 黑客基金会 以及 EXIN 网络和 IT 安全基金会马德里
- 获得以下专业证书的CAM专家认证培训师: 计算机安全 (IFCT0190)、语音和数据网络管理 (IFCM0310)、部门网络管理 (IFCT0410)、电信网络警报管理 (IFCM0410)、语音和数据网络运营商 (IFCM0110) 和互联网服务管理 (IFCT0509)
- 巴利阿里群岛大学外部合作者CSO/SSA (首席安全官/高级安全架构师)
- 马德里毕业于阿尔卡拉德埃纳雷斯大学的生物学专业
- DevOps领域的大师: Docker 和 KubernetesCas-培训
- 微软 Azure 安全技术E-Council



## 教师

### Catalá Barba, José Francisco 先生

- ◆ 电子技术员 网络安全专家
- ◆ 移动应用程序开发人员
- ◆ 西班牙国防部中级指挥部电子技术员
- ◆ 在位于巴伦西亚的福特工厂担任电子技术员

### Jiménez Ramos, Álvaro 先生

- ◆ 网络安全分析师
- ◆ The Workshop 高级安全分析师
- ◆ Axians 网络安全分析师 L1
- ◆ Axians 网络安全分析师 L2
- ◆ SACYR S.A. 的网络安全分析师
- ◆ 马德里理工大学远程信息处理工程学士
- ◆ CICE 网络安全和道德黑客硕士
- ◆ Deusto Training 的高级网络安全课程



### Marcos Sbarbaro, Victoria Alicia 女士

- B60。的原生 Android 移动应用程序开发人员英国
- 负责管理、协调和记录虚拟化安全警报环境的分析程序员
- 自动取款机 Java 应用程序分析员
- 签名验证和文件管理应用软件 开发专业人员
- 负责设备迁移、掌上电脑移动 设备 管理、维护和 培训的 系统技术员
- 加泰罗尼亚开放大学的计算机系统技术工程专业
- 新技术专业学院 CICE 的官方 EC-Council 和 CompTIA 计算机安全和道德黑客硕士课程

### Peralta Alonso, Jon 先生

- 阿尔蒂亚高级数据保护和网络安全顾问
- Arriaga Asociados Asesoramiento Jurídico y Económico S.L. 律师/法律顾问
- 专业公司的法律顾问/实习生: Óscar Padura
- 巴斯克公立大学法律学位
- EIS 创新学校数据保护硕士课程代表
- 巴斯克公立大学宣传硕士学位
- 卡斯蒂利亚伊莎贝尔一世国际大学民事诉讼实践专业硕士学位
- 个人数据保护、网络安全和信息通信技术法硕士学位讲师







### Redondo, Jesús Serrano 先生

- 网络开发和网络安全技术员
- 帕伦西亚 Roams 网络开发人员
- 马德里西班牙电信公司 前端开发 员
- 马德里 Best Pro Consulting SL 前端开发 员
- 卡斯蒂利亚-莱昂齐纳集团电信设备和服务安装工
- 卡斯蒂利亚-莱昂 Lican Comunicaciones SL 电信设备和服务安装工
- 由马德里Getafe CFTIC颁发的信息安全证书
- 由巴伦西亚Trinidad Arroyo IES颁发的高级电信与信息系统技术员
- 帕伦西亚特立尼达阿罗约 IES 中压和低压电工安装高级技师
- Incibe黑客学院提供的逆向工程、速记和加密培训

“

TECH精心挑选了这个课程的教学团队,以便你能从当今最好的专家那里学到东西”

# 10

# 对你事业的影响

完成这个网络安全管理 MBA(首席信息安全官) 将为网络安全局 (CISO首席信息安全官) 商学院校级硕士商业专业人士的资格增加一个质量的加分项, 提供所有的知识, 虽然这些知识看起来与他们的日常工作完全遥远, 但对于控制那些可能藏有一些影响整个组织的有害外部因素的计算机程序非常有用。出于这个原因, 在这个领域的更高专业性是不可避免的, 不仅对学生的个人和职业发展, 而且对他们工作的公司也是如此。







“

TECH将其所有的学术资源提供给学生使用, 以便他们获得必要的技能, 引导他们走向成功”

## 你准备好飞跃了吗？ 卓越的职业提升在等着你

TECH 科技大学 的网络安全管理 MBA (首席信息安全官) 课程是一个高强度且极具价值的项目, 旨在提升学员在这一广泛竞争领域的职业技能。这无疑是一个独特的机会, 可以提高专业水平, 也可以提高个人水平, 因为这涉及到努力和奉献。

提高自己学生专业水平上实现积极的变化, 并与最好的人交流, 这里就是你的地方在TECH。

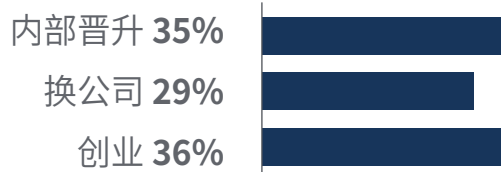
一个具有高学术水平的方案, 引领你的职业生涯走向成功。

完成这个 MBA 课程后, 学生可以获得必要的竞争力, 在职业生涯中进行彻底的改变。

### 改变的时候到



### 改变的类型



## 工资提高

---

完成这个课程后, 我们学生的工资会增长超过**25.22%**



# 11

# 对你公司的好处

网络安全管理 MBA (CISO, 首席信息安全官) 通过对高水平领导人的专业化培养, 有助于将组织的人才提高到最大的潜力。通过这种方式, 商业专业人士将能够通过掌握必要的技能, 自己控制网络安全进程, 为公司带来更多的质量。一个适合学生获得必要工具的计划, 他们随后可以在日常实践中应用这些工具, 为他们的公司带来巨大利益。







“

对于希望监测和管理潜在的网络安全问题的商业专业人员来说, 这是一个必备的方案”

培养和留住公司的人才是最好的长期投资。

01

### 人才和智力资本的增长知识资本

该专业人员将为公司带来新的概念、战略和观点,可以为组织带来相关的变化。

---

02

### 留住高潜力的管理人员,避免人才流失

这个计划加强了公司和经理人之间的联系,并为公司内部的职业发展开辟了新的途径。

03

### 培养变革的推动者

你将能够在不确定和危机的时候做出决定,帮助组织克服障碍。

---

04

### 增加国际扩张的可能性

由于这一计划,该公司将与世界经济的主要市场接触。



05

### 开发自己的项目

可以在一个真实的项目上工作, 或在其公司的研发或业务发展领域开发新。

---

06

### 提高竞争力

该课程将使学生具备接受新挑战的技能, 从而促进组织的发展。

# 12 学位

网络安全管理 MBA (CISO, 首席信息安全官) 商学院校级硕士除了保证最严格和最新的培训外, 还可以获得由 TECH 科技大学 颁发的商学院校级硕士学位证书。



“

顺利完成这个课程并获得大学学位, 无需旅行或通过繁琐的程序”

这个网络安全管理 MBA (CISO, 首席信息安全官) 商学院校级硕士包含了市场上最完整和最新的课程。

评估通过后, 学生将通过邮寄收到TECH科技大学颁发的相应的商学院校级硕士学位。

学位由TECH科技大学颁发, 证明在商学院校级硕士学位中所获得的资质, 并满足工作交流, 竞争性考试和职业评估委员会的要求。

学位: 网络安全管理 MBA (CISO, 首席信息安全官) 商学院校级硕士

模式: 在线

时长: 12个月



\*海牙加注。如果学生要求为他们的纸质资格证书提供海牙加注, TECH EDUCATION将采取必要的措施来获得, 但需要额外的费用。





商学院校级硕士  
网络安全管理 MBA  
(CISO, 首席信息安全官)

- » 模式:在线
- » 时长: 12个月
- » 学位: TECH 科技大学
- » 课程表:自由安排时间
- » 考试模式:在线

商学院校级硕士  
网络安全管理 MBA  
(CISO, 首席信息安全官)

