大学课程
智能手机的网络安全

tech 科学技术大学

tech 科学技术大学

大学课程
智能手机的网络安全

- 模式:**在线**
- 时间:**6周**
- 学历:**TECH科技大学**
- 时间表:**按你方便的**
- 考试:**在线**

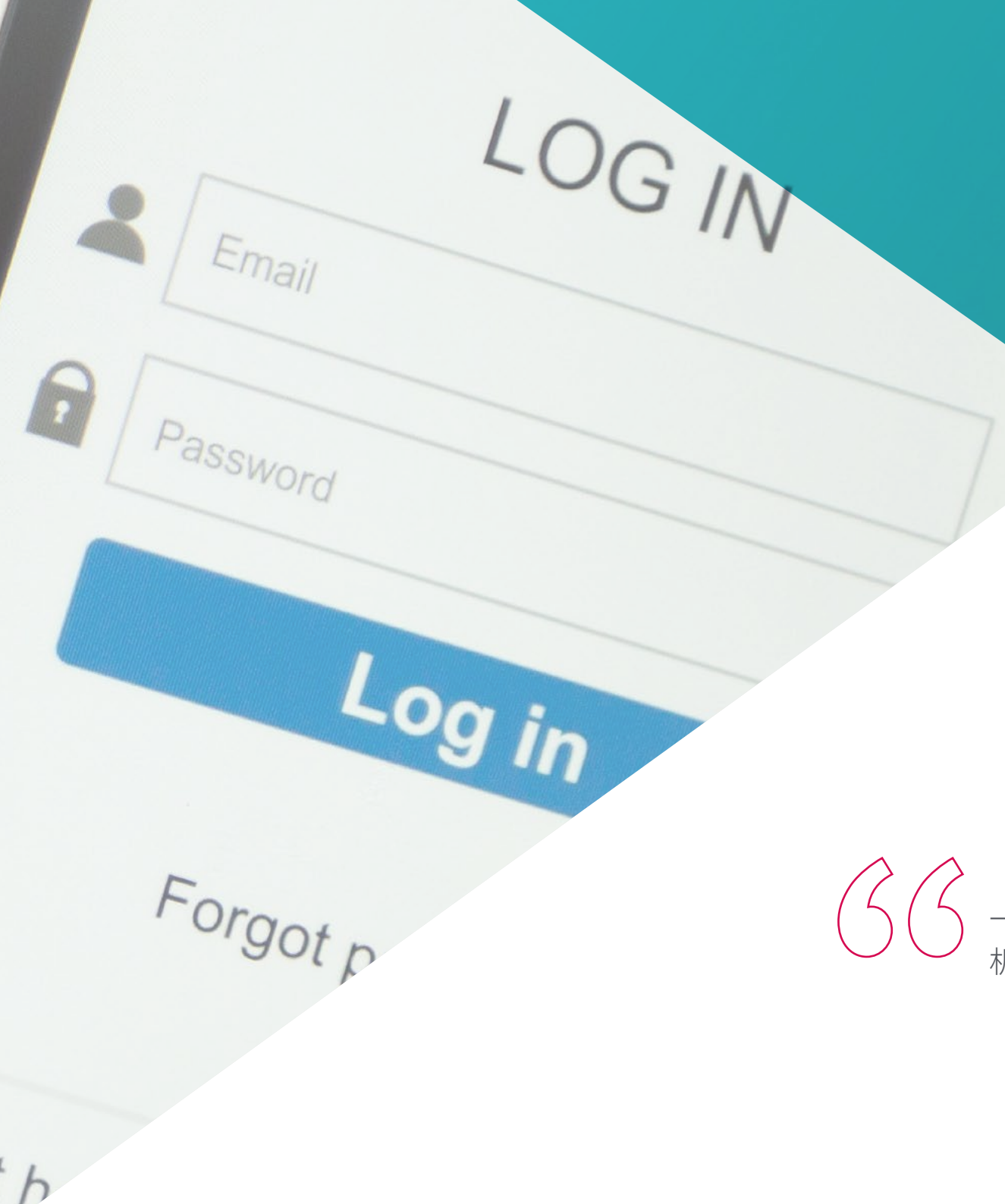
网络访问: www.techtitute.com/cn/information-technology/postgraduate-certificate/smartphone-cybersecurity

目录

01

介绍

使用移动设备迫使用户在保护其个人数据方面承担一定的风险，在某些情况下，风险可能非常高。这些设备、手机或平板电脑的智能化程度不断提高，也增加了与之相关的攻击面，打开了新的漏洞，可能变成犯罪，甚至是身份盗窃、抢劫或欺诈。为了应对这种情况，网络安全专业人员被迫与风险的出现同步工作，不断开发保护性的反应。该计划是为专业人士提供该领域最新信息的工具，以使他们能够提供有效和创新的解决方案。



一门大学课程，将为你提供打击智能手机上的网络攻击的最创新和最新的工具"

我们生活在一个移动设备的使用越来越广泛的时代。手机早已不再是单纯的电话，而成为一台小型计算机，能够随时浏览互联网，运行各种应用程序，在地图上定位我们的位置，绘制路线，存储内部和外部的数据，等等。当我们谈论这些设备时，我们不仅指的是手机，还包括平板电脑。两者都是为使我们的生活更轻松而设计和准备的设备。感谢它们的存在，我们可以轻松地移动，并在任何时候都可以访问网络，还可以拥有越来越流行的云服务。

我们不能忘记，由于所有这些 "智能"，这些设备的攻击面已经从0成倍地增加到100，这些设备的大量使用使它们成为一个容易的目标。移动设备现在是攻击者的主要目标，他们试图侵犯隐私、窃取身份、窃取数据、未经用户同意获得访问权并利用这些设备的所有者进行犯罪。

因此，我们必须而且绝对有必要采取一切可以利用的措施来保护我们的隐私。没有100%的安全，但如果我们知道我们所面临的攻击类型，我们所面临的风险，并拥有应对这些风险所需的信息，我们将采取一个重要的步骤，为我们的信息增加另一层安全。

这个**智能手机的网络安全大学课程**包含市场上最完整和最新的课程。主要特点是：

- 制定由网络安全专家提出的案例研究
- 该书的内容图文并茂、示意性强、实用性强为那些视专业实践至关重要的学科提供了科学和实用的信息
- 实际练习，你可以进行自我评估过程，以改善你的学习
- 其特别强调创新方法
- 理论课、向专家提问、关于有争议问题的讨论区和个人反思性论文
- 可以从任何有互联网连接的固定或便携式设备上获取内容

> 获得必要的知识，在短短几周的工作中开发一个有效的分层保护系统"

专业人士需要的信息，以创建保护系统，保证在使用智能手机时的安全，在一个高度合格的方案中"

通过以实践为重点的大学课程学习，将你的能力提高到专家水平。

一个高度熟练的过程，创建了可管理和灵活的，最有趣的在线教学方法。

该课程的教学人员包括来自该行业的专业人士，他们将自己的工作经验带到了这一培训中，还有来自领先公司和著名大学的公认专家。

多媒体内容是用最新的教育技术开发的，将允许专业人员进行情景式学习，即一个模拟的环境，提供一个身临其境的培训，为真实情况进行培训。

该课程的设计重点是基于问题的学习，通过这种方式，专业人员必须尝试解决整个学年出现的不同专业实践情况。为此，它将得到一个由公认的专家制作的互动视频的创新系统的支持。

02

目标

智能手机的网络安全大学课程为学生提供了快速和轻松地在这个领域工作的能力。通过现实的和非常有趣的目标，这个学习过程已经被配置为逐步引导学生获得必要的理论和实践知识，以进行高质量的干预，此外，发展横向能力，使他们能够通过阐述调整和精确的反应来面对复杂的情况。

通过卓越的教学质量过程，将你的技能用于充满工作机会的领域"

总体目标

- 分析当前主要的移动平台、特点和用途
- 检查现有的漏洞和威胁，以及主要的攻击载体
- 了解如何评估与公司内外漏洞相关的风险
- 确定工具和最佳实践指南，以实现对移动设备的保护

> 考虑到学生，这门大学课程实施了目前最有趣的学习支持系统"

具体目标

- 检查各种攻击向量以避免成为容易的目标
- 确定移动设备用户面临的主要攻击和恶意软件类型
- 分析最新设备以在配置中建立更高的安全性
- 指定在 iOS 平台和 Android 平台上执行渗透测试的主要步骤
- 发展有关不同保护和安全工具的专业知识
- 建立面向移动设备的良好编程实践

03

课程管理

教授该课程的教师都是因其在该领域的卓越能力而被选中的。他们将技术和实践经验与教学经验相结合，为学生实现其目标提供一流的支持。通过它们，该方案对这一领域的干预的真实特征提供了最直接和最直接的视野，实现了最大利益的背景视野。

智能手机的网络安全方面的专家讲师将陪伴你完成每个阶段的学习，让你对这项工作有最真实的认识"

国际客座董事

Frederic Lemieux博士被国际公认为智能、国家安全、内部安全、网络安全和颠覆性技术领域的创新专家和鼓舞人心的领袖。他在研究和教育方面的持续奉献和重要贡献使他成为当今促进安全和新兴技术理解的关键人物。在他的职业生涯中，他构想并领导了一流的学术项目，包括**蒙特利尔大学、乔治·华盛顿大学**和**乔治敦大学**等知名机构。

在他丰富的经验中，他发表了许多与**犯罪情报、警务工作、网络威胁和国际安全**相关的重要书籍。此外，他在**网络安全**领域做出了重大贡献，发表了多篇学术文章，其中探讨了在重大灾难期间的犯罪控制、反恐怖主义、情报机构和警务合作。此外，他还在各种国内和国际会议上担任了小组讨论嘉宾和主要发言人，成为学术和职业领域的权威。

Frederic Lemieux博士曾在不同的学术、私人和政府组织中担任编辑和评审角色，反映了他在自己专业领域的影响力和承诺卓越。因此，他杰出的学术生涯使他担任了**乔治敦大学**的**应用情报、网络安全风险管理、技术管理和信息技术管理**MPS项目的实践教授和院长。

Lemieux, Frederic 医生

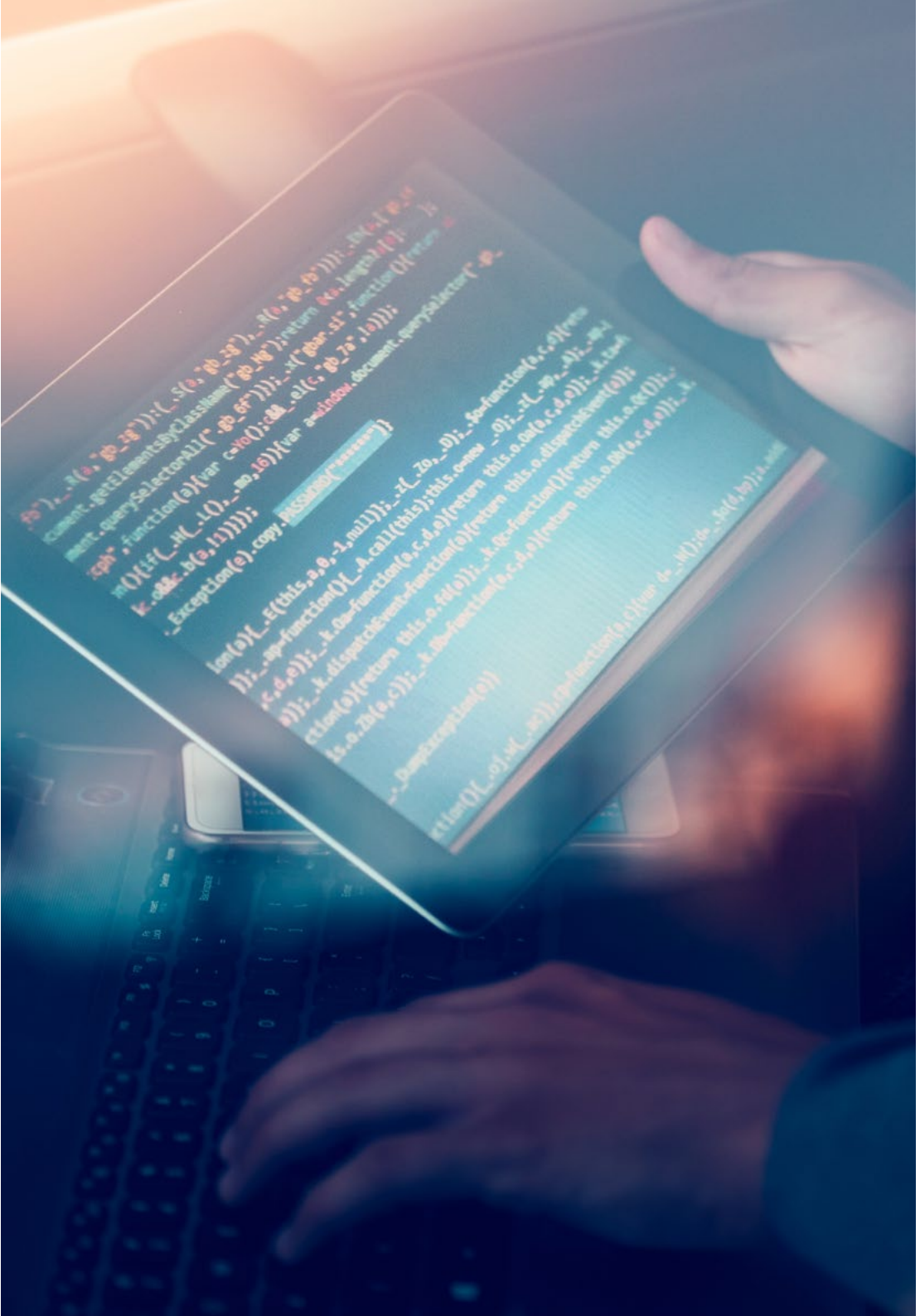
- 乔治敦大学情报、网络安全和颠覆性技术研究员
- 乔治城大学信息技术管理硕士课程主任
- 乔治城大学技术管理硕士课程主任
- 乔治城大学网络安全风险管理硕士学位主任
- 乔治城大学应用智能硕士学位主任
- 乔治城大学实习教授
- 蒙特利尔大学犯罪学学院犯罪学博士
- 法国拉瓦尔大学社会学学士，辅修心理学
- 成员：
- 乔治城大学新项目圆桌会议委员会

> 感谢 TECH，您将能够与世界上最优秀的专业人士一起学习”

管理人员

Fernández Sapena, Sonia 女士

- 计算机安全和道德 黑客 培训师赫塔菲国家计算机和电信中心马德里
- 认证的电子理事会讲师马德里
- 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）
- 外部合作者 CSO/SSA（首席安全官/高级安全架构师）巴利阿里群岛大学
- 计算机工程师阿尔卡拉-德-埃纳雷斯大学。马德里
- DevOps 硕士：Docker 和 KubernetesCas-培训马德里
- 微软 Azure 安全技术。E 理事会马德里



教师

Marcos Sbarbaro, Victoria Alicia 女士

- B60 。的原生 Android 移动应用程序开发人员UK (英国)
- 用于客户端安全警报虚拟化环境的管理、协调和文档编制的程序员分析师
- 客户端 ATM 的Java 应用程序程序员分析师。
- 用于客户签名验证和文档管理应用程序的软件开发专家
- 用于客户签名验证和文档管理应用程序的软件开发专家
- 计算机系统的技术工程。加泰罗尼亚开放大学。
- 计算机安全和道德 黑客硕士。来自新技术专业学校 CICE 官方 EC-Council 和 CompTIA

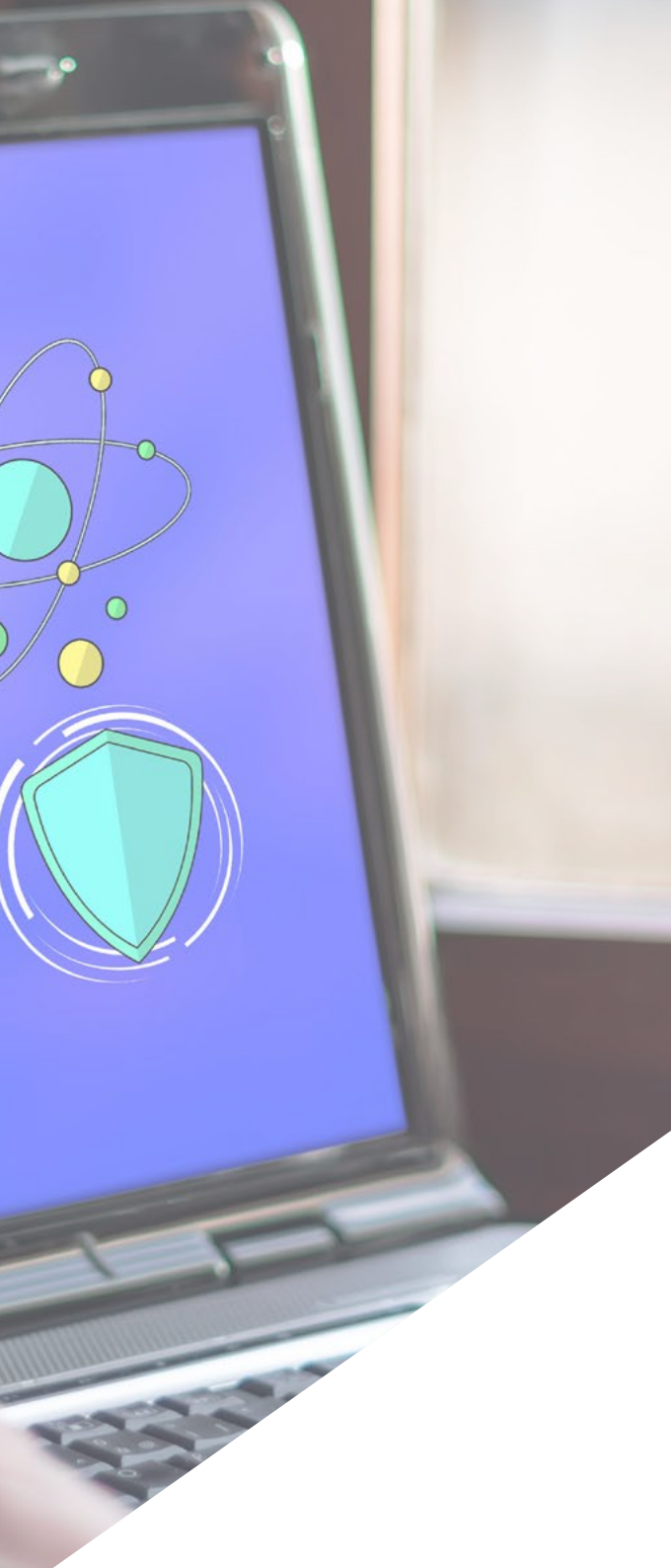
Catalá Barba, José Francisco 博士

- MINISDEF中的中间指令。管理 GOE III 中的不同任务和职责，例如内部网络的管理和事件管理、针对不同领域的定制计划的实施、网络用户和一般集团员工的培训课程
- 位于瓦伦西亚 Almussafes 的福特工厂的电子技术员，编程机器人、PLC、维修和保养
- 电子技术员
- 移动应用程序开发人员

04

结构和内容

通过本课程不同主题的进展，学生将能够获得开发智能手机安全系统所需的所有知识。它的结构是为了有效地获得补充性的学习，这将使学习的渗透和巩固已经学习的内容，为学生提供尽快介入的能力。这是一个高强度、高质量的课程，旨在培训该行业的精英。



智能手机网络安全干预的所有方面以一种注重效率的研究方法有条不紊地发展"

模块1.智能手机的 安全

1.1. 移动设备的世界
- 1.1.1. 移动平台类型
- 1.1.2. iOS 设备
- 1.1.3. 安卓设备

1.2. 移动安全管理
- 1.2.1. OWASP 移动安全项目
  - 1.2.1.1. 十大漏洞
- 1.2.2. 通信、网络和连接模式

1.3. 商业环境中的移动设备
- 1.3.1. 风险
- 1.3.2. 安全政治
- 1.3.3. 设备监控
- 1.3.4. 移动设备管理 (MDM)

1.4. 用户隐私和数据安全
- 1.4.1. 信息状态
- 1.4.2. 数据保护和保密
  - 1.4.2.1. 许可权
  - 1.4.2.2. 加密
- 1.4.3. 安全数据存储
  - 1.4.3.1. iOS 的安全存储
  - 1.4.3.2. 安卓的安全存储
- 1.4.4. 应用程序开发中的正确做法

1.5. 漏洞和攻击媒介
- 1.5.1. 漏洞
- 1.5.2. 攻击向量
  - 1.5.2.1. 恶意软件
  - 1.5.2.2. 泄露数据
  - 1.5.2.3. 操作数据

1.6. 主要威胁
- 1.6.1. 用户未强制
- 1.6.2. 恶意软件
  - 1.6.2.1. 恶意软件的类型
- 1.6.3. 社会工程学
- 1.6.4. 数据泄露
- 1.6.5. 信息盗窃
- 1.6.6. 不安全的 Wi-Fi 网络
- 1.6.7. 过时的软件
- 1.6.8. 恶意应用程序
- 1.6.9. 弱密码
- 1.6.10. 安全设置薄弱或不存在
- 1.6.11. 物理访问
- 1.6.12. 丢失或被盗的设备
- 1.6.13. 身份冒充(诚信)
- 1.6.14. 弱或损坏的密码学
- 1.6.15. 拒绝服务 (DoS)

1.7. 主要攻击
- 1.7.1. 网络钓鱼攻击
- 1.7.2. 与通信模式相关的攻击
- 1.7.3. 网络钓鱼攻击
- 1.7.4. 加密劫持攻击持攻击
- 1.7.5. 中间人攻击

1.8. 黑客攻击
- 1.8.1. Rooting 和Jailbreaking
- 1.8.2. 移动攻击剖析
  - 1.8.2.1. 威胁传播
  - 1.8.2.2. 在设备上安装恶意软件
  - 1.8.2.3. 持久性
  - 1.8.2.4.有效载荷执行和信息提取
- 1.8.3. 入侵 iOS 设备:机制和工具
- 1.8.4. 入侵 Android 设备:机制和工具

1.9. 渗透测试
- 1.9.1. iOS 渗透测试
- 1.9.2. 安卓 渗透测试
- 1.9.3. 工具

1.10. 保护和安全
- 1.10.1. 安全设定
  - 1.10.1.1. iOS 设备
  - 1.10.1.2. 安卓设备
- 1.10.2. 安防措施
- 1.10.3. 保护工具

> 所有的分析、发展和智能手机的保护工具都是一个非常有趣和热门的主题"

05

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:**再学习**。

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。

发现再学习，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”

案例研究,了解所有内容的背景

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”

你将进入一个以重复为基础的学习系统,在整个教学大纲中采用自然和渐进式教学。

学生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。

一种创新并不同的学习方法

该技术课程是一个密集的教学计划，从零开始，提出了该领域在国内和国际上最苛刻的挑战和决定。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技术基础，确保遵循当前经济，社会和职业现实。

> 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”

在世界顶级计算机科学学校存在的时间里，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对的问题，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的案例。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。

再学习方法

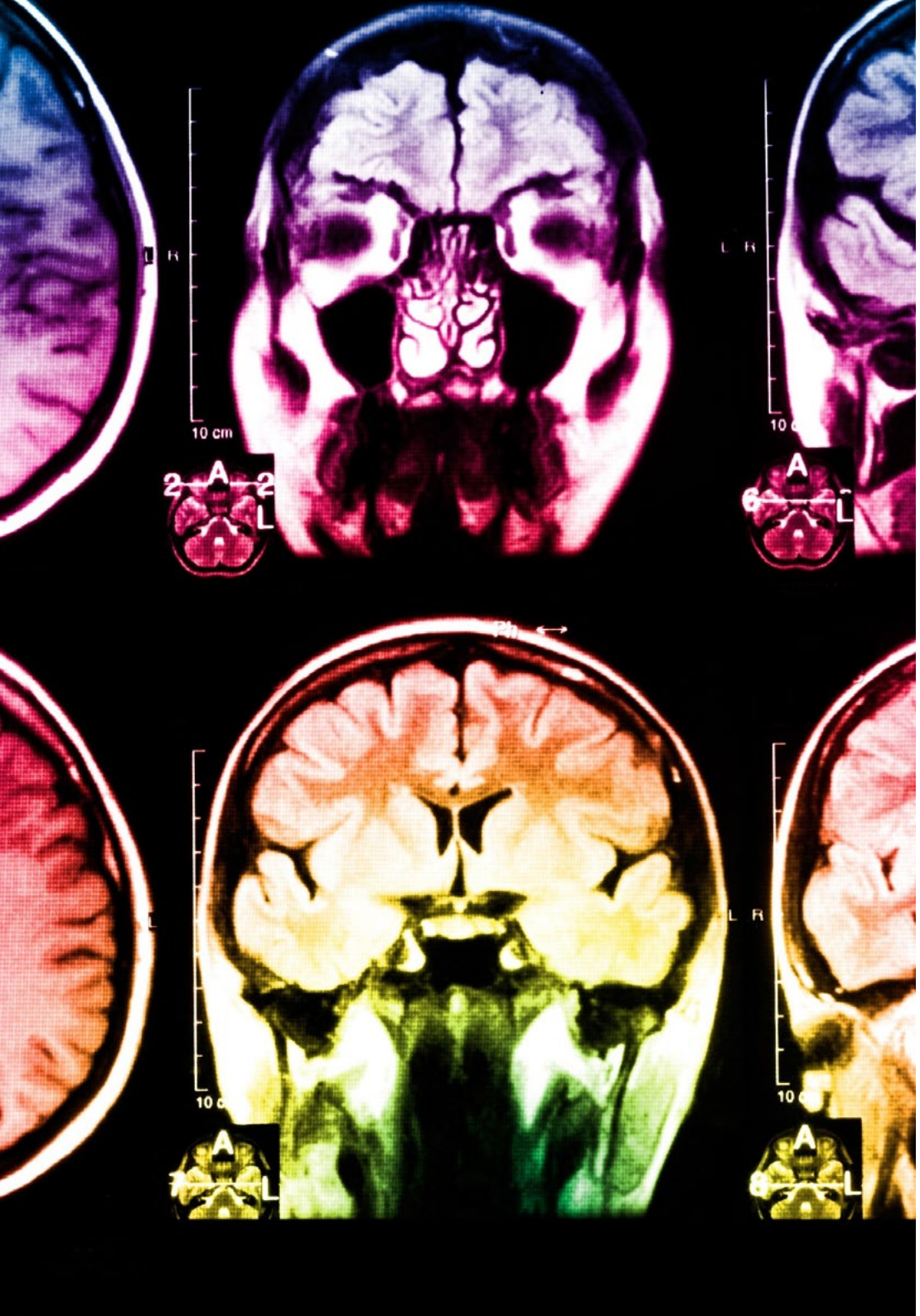
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

我们用最好的100%在线教学方法加强案例研究：再学习。

> 在2019年，我们取得了世界上所有西班牙语在线大学中最好的学习成绩。

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再学习。

我校是唯一获准使用这一成功方法的西班牙语大学。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。

再学习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。

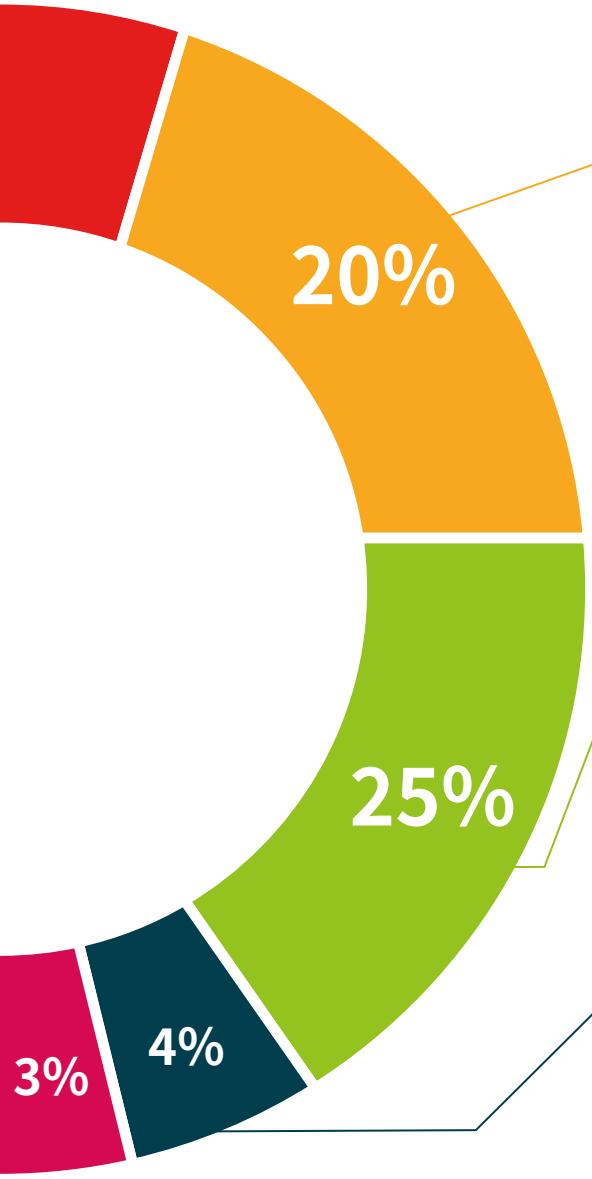
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

技能和能力的实践

你将开展活动以发展每个学科领域的具体能力和技能。在我们所处的全球化框架内，我们提供实践和氛围帮你取得成为专家所需的技能和能力。

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。由国际上最好的专家介绍,分析和辅导案例。

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丸中,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。

06

学历

智能手机的网络安全大学课程除了保证最严格和最新的培训外，还可以获得由TECH科技大学颁发的大学课程学位证书。

成功地完成这个课程并获得大学学位，而无需旅行或繁文缛节的麻烦"

这个**智能手机的网络安全大学课程**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**大学课程**学位。

TECH科技大学颁发的证书将表达在大学课程获得的资格，并将满足工作交流，竞争性考试和专业职业评估委员会的普遍要求。

学位：**智能手机的网络安全大学课程**

官方学时：**150小时**


tech 科学技术大学

授予

文凭

_____先生/女士，身份证号码_____

顺利通过并获得认证的课程是

大学课程

智能手机的网络安全

这是一个由本大学授予的学位，相当于150个小时，
开始日期是 dd/mm/aaaa,结束日期是dd/mm/aaaa。

截至2018年6月28日，TECH是一所被公共教育部认可的私立高等教育机构。

2020年六月17日

Tere Guevara Navarro女士
校长

Unique TECH Code: AFWORD23S techtitute.com/certificates

*海牙认证。如果学生要求有海牙认证的毕业证书，TECH EDUCATION将作出必要的安排，并收取额外的费用。

tech 科学技术大学

大学课程
智能手机的网络安全

- 模式:在线
- 时间:6周
- 学历:TECH科技大学
- 时间表:按你方便的
- 考试:在线

大学课程
智能手机的网络安全

tech 科学技术大学