大学课程
法证基础和 DFIR

tech 科学技术大学

tech 科学技术大学

大学课程
法证基础和 DFIR

- 模式:**在线**
- 时长: **6周**
- 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/information-technology/postgraduate-certificate/forensic-fundamentals-dfir

目录

01

介绍

随着计算机系统等新技术的发展，各机构在互联网上的存在越来越多。然而，随着网络攻击的增加，企业面临着各种挫折。在这方面，如果黑客进入你的网络，他们可能会删除敏感数据，甚至索要赎金，以换取释放被封锁的系统。因此，公司必须聘请法证基础知识专家来检测安全漏洞并尽可能减少其影响。为满足这一需求，TECH 正在启动一项创新计划，以采用先进的数字证据分析技术。此外，这个课程 100%在线教学，保证了学生的便利性。

你是否想分析防火墙日志，从而检测网络入侵?感谢了这次培训，我只用了 150 个小时就完成了任务"

企业越来越意识到在组织中配备网络安全 IT 专家的重要性。这样做的好处包括保护你的数字资产和进行取证调查，以确定潜在事件的原因和程度。反过来，这些专业人员也会收集可作为法庭证据和起诉网络罪犯的信息。在这方面，它们甚至可以帮助组织遵守数据安全法规和安全漏洞通知要求。

面对这种情况，TECH 正在开发最先进的培训，使学生能够通过实施最适当的策略来防止黑客攻击。学术行程将以监管链为基础，深入探讨获取证据的过程。通过这种方式，学生将充当计算机取证实验室，解决影响组织的事件。此外，这个课程还将涉及网络数据包分析，因此学生将进行 防火墙日志记录。还将提供恶意软件，以便执行反汇编技术。
毕业生将运用 DFIR 方法，释放自己的创造力，提供最具创新性的业务解决方案。

此外，为了巩固对教学内容的掌握，本教学大纲采用了 Relearning系统。值得注意的是，TECH 是使用这种教学模式的先驱，它通过自然和渐进的重复来促进对复杂概念的吸收。在这方面，该计划还利用了各种形式的材料，如互动摘要或解释性视频。所有这些都采用方便的 100% 在线模式，学生可以根据自己的职责调整时间安排。

这个**法证基础和 DFIR大学课程**包含市场上最完整和最新的课程。主要特点是：

- 由法医基础和 DFIR 专家介绍案例研究的发展情况
- 这个课程的图形化、示意图和突出的实用性内容提供了关于那些对专业实践至关重要的学科的最新和实用信息
- 可以进行自我评估过程的实践，以推进学习
- 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这个反思性论文
- 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

> 你将在《福布斯》评选的全球最佳数字大学中制定事件响应课程"

需要从损坏的介质中恢复数据?TECH为你提供实现这一目标的最佳工具。

“通过 TECH 的教学工具(包括讲解视频和互动摘要),你将实现自己的目标”

你将撰写法医报告,并在重要的法庭案件中作为专家证人出庭。

这个课程的教学人员包括来自这个行业的专业人士,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。

它的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。

这个课程的设计重点是基于问题的学习,藉由这种学习,专业人员必须努力解决整个学年出现的不同的专业实践情况。为此,你将获得由知名专家制作的新型交互式视频系统的帮助。

02

目标

该课程的设计将探索收集和分析数字证据的先进技术，解决安全漏洞问题。这样，学生就能学到更多档案分析和保管链保护方面的知识。此外，学生还将研究最有效的策略，以最大限度地减少潜在网络事件的影响。

忘掉背书!通过 Relearning 系统你将以自然、渐进的方式将概念融会贯通”

总体目标

- 掌握渗透测试和红队模拟的高级技能，识别并利用系统和网络中的漏洞
- 培养协调进攻型网络安全专业团队的领导技能，优化 Pentesting 和Red Team项目的执行
- 培养分析和开发恶意软件的技能，了解其功能并应用防御和教育策略
- 通过编写详细的技术和执行报告，向技术和执行受众有效地介绍研究结果，磨练沟通技能
- 促进网络安全领域的道德和责任实践，在所有活动中考虑道德和法律原则
- 让学生了解网络安全领域的最新趋势和技术

> 工业网络安全领域的杰出专业人员将为你提供支持"

具体目标

模块 1. 法证基础和 DFIR

- 扎实了解数字取证调查 (DFIR) 的基本原则及其在解决网络事件中的应用
- 培养安全和取证数字证据的技能，确保保管链得到保护
- 学习如何对文件系统进行取证分析
- 使学生熟悉日志和日志分析的高级技术，从而能够重建数字环境中的事件
- 学习如何在破案过程中应用数字取证调查方法，从识别到记录调查结果
- 使学生熟悉数字证据分析和 Pentesting环境中法医技术的应用
- 培养编写详细、清晰的法医报告的技能，以易于理解的方式介绍调查结果和结论
- 促进与事件响应 (IR) 团队的有效合作，优化威胁调查和缓解方面的协调
- 促进数字取证方面的道德和法律实践，确保遵守网络安全法规和行为标准

03

课程管理

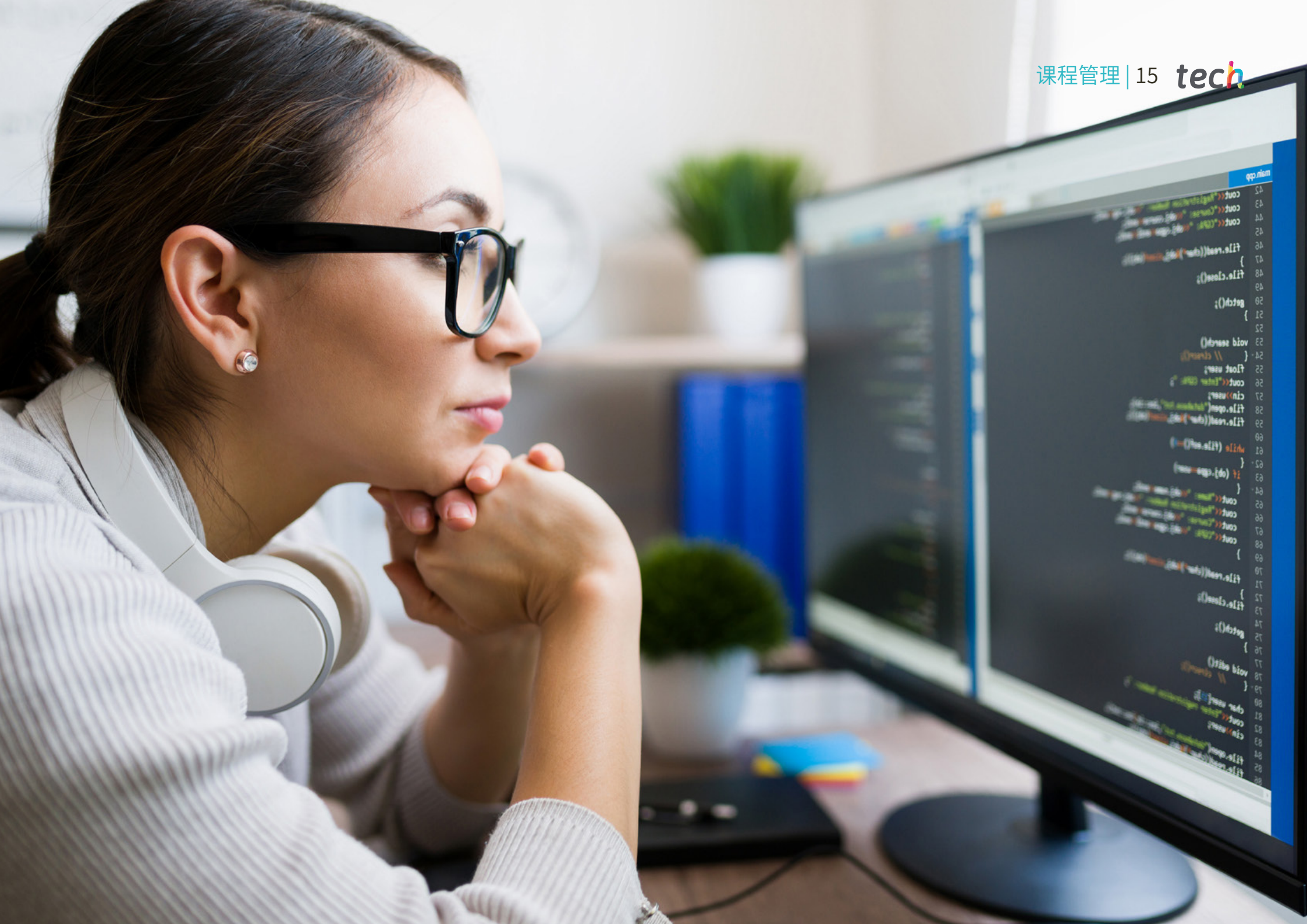
TECH 致力于提供卓越的教育，其专业人员在国际上享有盛誉。这些网络安全专业人员拥有丰富的网络安全背景，因此本培训为学生掌握基本的数字取证调查和事件响应技能提供了最有效的工具。这样，学生们就能在提供大量就业机会的数字行业中获得所需的专业保障。

图书馆拥有大量不同视听格式的多媒体资源"

管理人员

Gómez Pintado, Carlos 先生

- 网络安全和网络团队 Cipherbit 经理（Grupo Oesía
- Wesson App 管理顾问兼投资者
- 马德里理工大学软件工程与信息社会技术专业毕业
- 与教育机构合作开发网络安全 **高级培训周期**



04

结构和内容

议程将包括旨在立即应对网络事件、减少其影响和恢复正常运行的模拟。此外，该课程还深入分析了最重要的操作系统（Windows、Linux 和 maCos），使学生能够从损坏的介质中恢复数据。还将进一步开展恶意软件分析，以识别恶意代码，从而防止组织遭受蠕虫或木马等病毒的侵害。这样，学生就能掌握扎实的数字取证知识。

图书馆拥有大量不同视听格式的多媒体资源"

模块 1. 法证基础和 DFIR

1.1. 数字取证
- 1.1.1. 计算机取证的历史和演变
- 1.1.2. 计算机取证在网络安全中的重要性
- 1.1.3. 计算机取证的历史和演变

1.2. 计算机取证基础知识
- 1.2.1. 监管链及其实施
- 1.2.2. 数字证据的类型
- 1.2.3. 证据获取过程

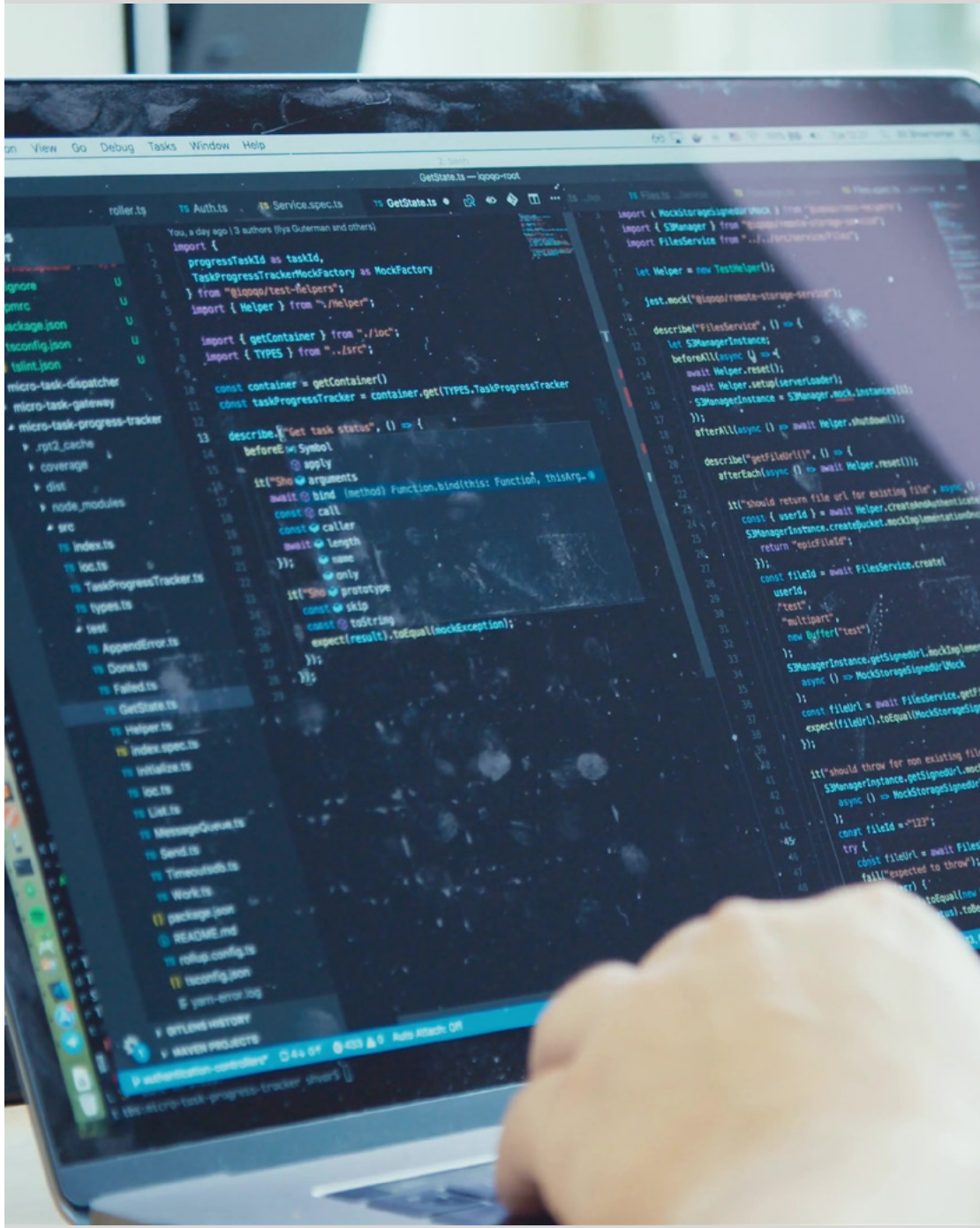
1.3. 文件系统和数据结构
- 1.3.1. 主要文件系统
- 1.3.2. 数据隐藏方法
- 1.3.3. 分析文件元数据和属性

1.4. 操作系统分析
- 1.4.1. Windows 系统的取证分析
- 1.4.2. Linux 系统的取证分析
- 1.4.3. 对 macOS 系统进行取证分析

1.5. 数据恢复和磁盘分析
- 1.5.1. 从受损介质中恢复数据
- 1.5.2. 磁盘分析工具
- 1.5.3. 文件分配表的解释

1.6. 网络和流量分析
- 1.6.1. 网络数据包捕获和分析
- 1.6.2. 分析防火墙日志
- 1.6.3. 网络入侵检测

1.7. 恶意软件和恶意代码分析
- 1.7.1. 恶意软件的分类及其特点
- 1.7.2. 静态和动态恶意软件分析
- 1.7.3. 反汇编和调试技术



1.8. 记录和事件分析
- 1.8.1. 系统和应用中的寄存器类型
- 1.8.2. 相关事件的解释
- 1.8.3. 记录分析工具

1.9. 应对安全事件
- 1.9.1. 事件响应流程
- 1.9.2. 制定事件响应计划
- 1.9.3. 与安全团队协调

1.10. 举证和法律
- 1.10.1. 法律领域的数字证据规则
- 1.10.2. 编写法医报告
- 1.10.3. 作为专家证人出庭

> 图书馆拥有大量不同视听格式的多媒体资源"

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: **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”

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。

Re-learning 方法

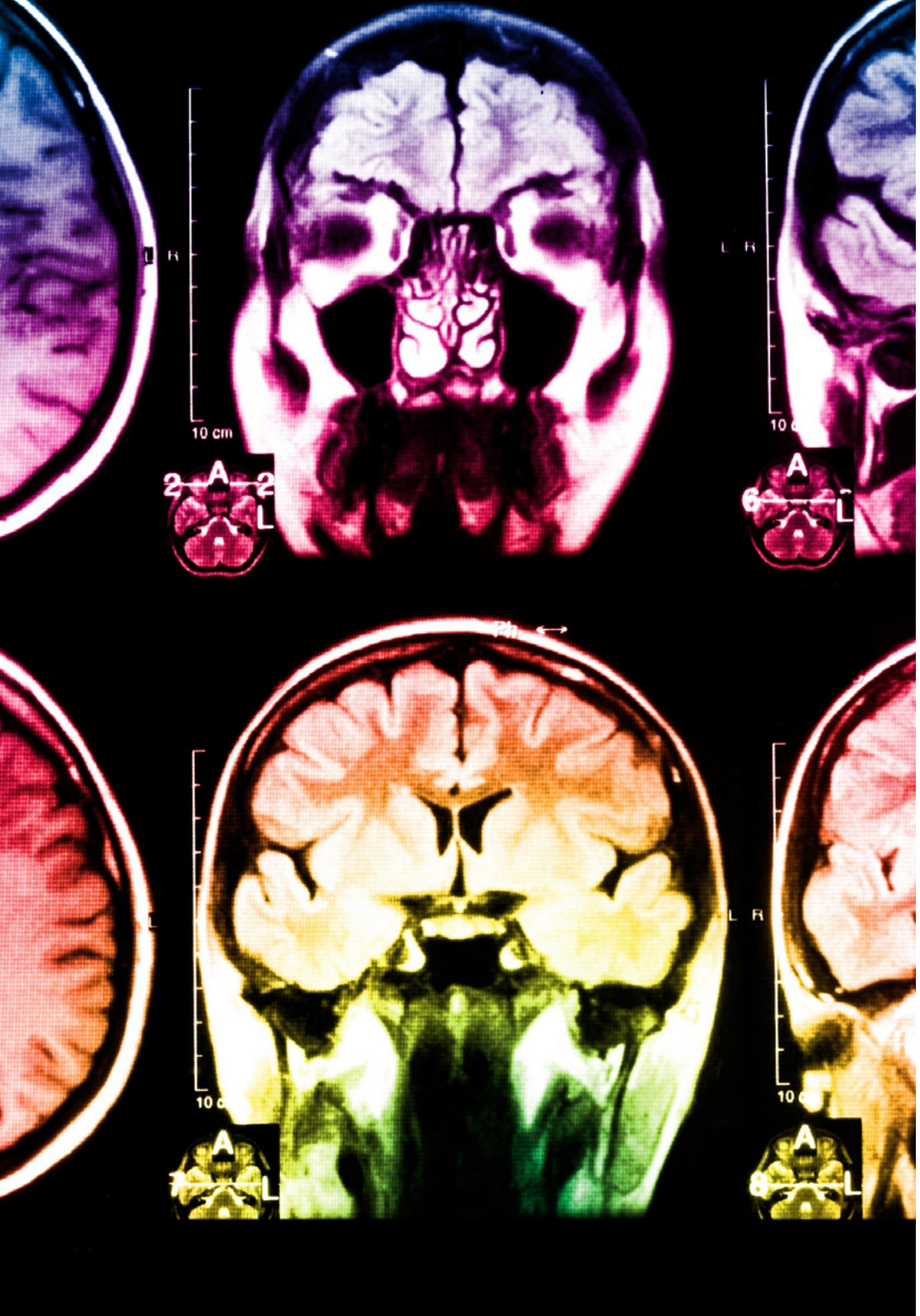
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

我们用最好的100%在线教学方法加强案例研究：Re-learning。

> 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 Re-learning。

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。

> 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。

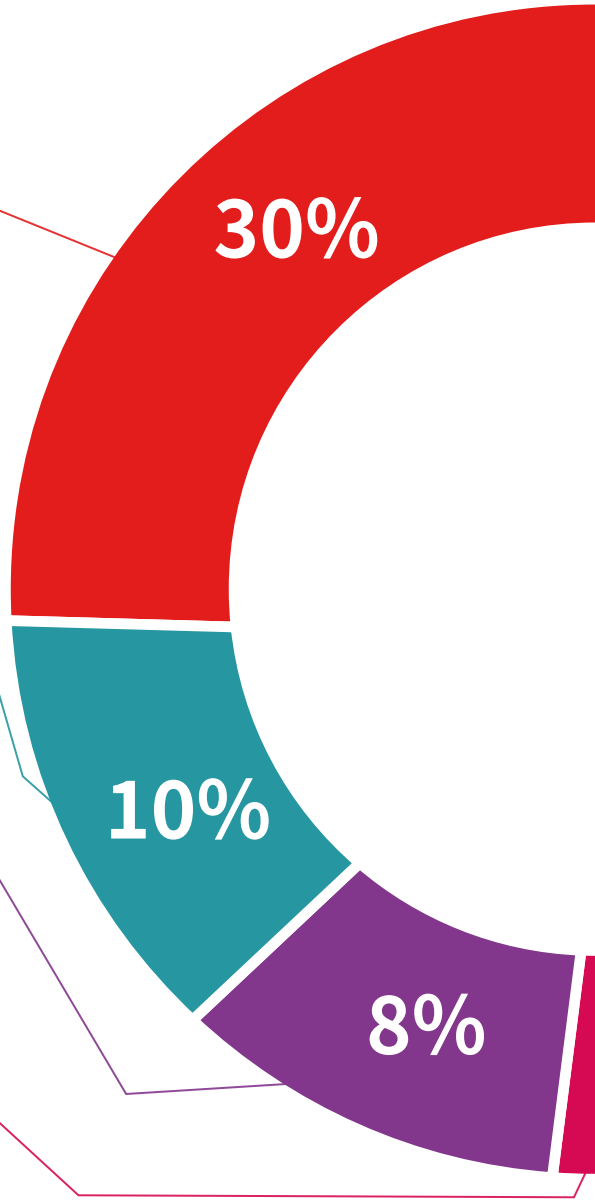
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

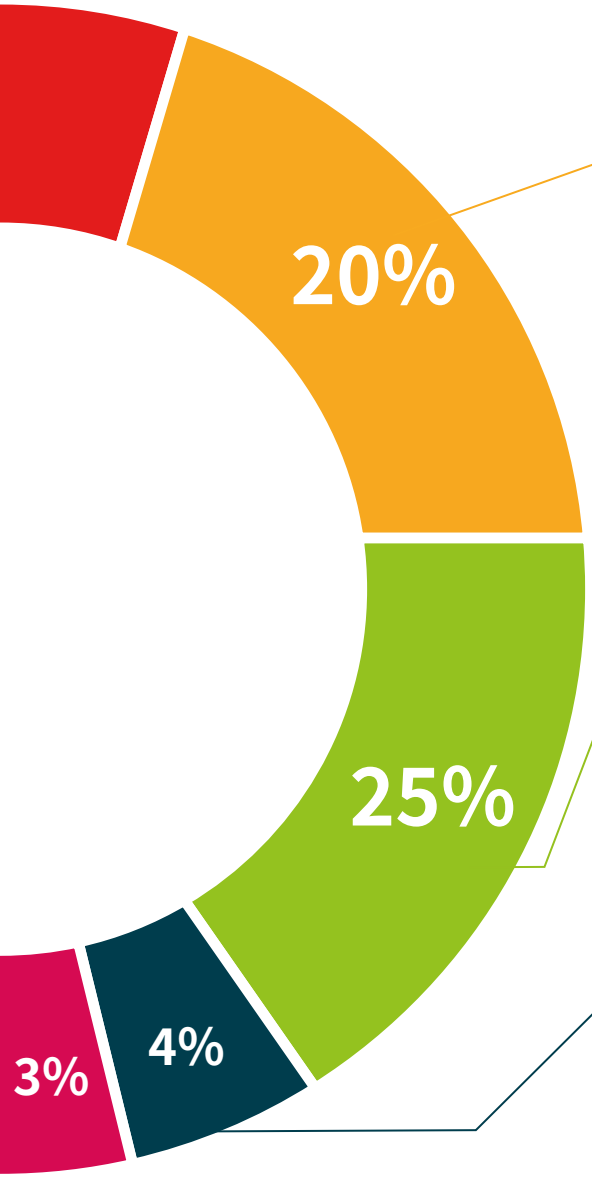
技能和能力的实践

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

学位

法证基础和 DFIR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。

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**法证基础和 DFIR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：**法证基础和 DFIR大学课程**

模式：**在线**

时长：**6周**


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

法证基础和 DFIR

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。

tech 科学技术大学

大学课程
法证基础和 DFIR

- 模式:**在线**
- 时长: **6周**
- 学位: **TECH 科技大学**
- 课程表:**自由安排时间**
- 考试模式:**在线**

大学课程
法证基础和 DFIR

tech 科学技术大学