专科文凭
信息科技安全管理

tech 科学技术大学

tech 科学技术大学

专科文凭

信息科技安全管理

- 模式:**在线**
- 时间:**6个月**
- 学历:**TECH科技大学**
- 时间:**16小时/周**
- 时间表:**按你方便的**
- 考试:**在线**

网络访问: www.techtitute.com/cn/information-technology/postgraduate-diploma/postgraduate-diploma-it-security-management

目录

01

介绍

信息科技在许多公司的整合产生了附带效应：信息科技安全的风险增加了。现在，企业需要了解可能影响其正常运作和服务的各种攻击和漏洞。因此，公司必须有一名专家负责管理这些科技的安全。该课程为专业人员提供了学习该领域最先进的 IT 保护方法的机会，因为它将提供基于业务参数的风险评估、身份和访问管理或入侵测试等方面的深入知识。

越来越多的公司需要 IT 安全管理方面的专家。该课程将使你在专业方面取得进步，更深入地了解与安全相关的业务连续性规划等问题"

事实是：几乎没有公司不在内部流程中使用数字和信息技术工具。目前，员工身份识别、物流系统或与供应商和客户的联系等活动和业务主要通过信息科技进行。但是，这些科技需要经过适当的设计和监控，因为它们可能被利用来获取数据或侵入公司的敏感领域。

因此，安全管理专家是一个需求量越来越大的职位，不是任何 IT 专家都能胜任的。要求具备考虑到网络安全最新发展的最新知识。因此，本专科文凭旨在为专业人员提供该领域的最新进展，深入探讨安全审计、终端设备安全或对不同事件的最有效回应等问题。

该课程还采用了 100% 在线的形式，以适应专业人员的情况，使他们能够随时随地以自己喜欢的方式学习。它还将拥有一支在网络安全领域享有盛誉的师资队伍，并辅以大量多媒体资源，使学习过程舒适、快捷、高效。

这个**信息科技安全管理专科文凭**包含市场上最完整和最新的课程。主要特点是：

- 由计算机专家提出的实际案例的网络安全发展
- 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
- 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

> 该计划将让你更深入地了解业务连续性计划的生命周期或脆弱性管理等方面"

TECH 为你提供最好的多媒体资源：案例研究、理论实践活动、视频、互动摘要等。所有这些都能使学习过程变得灵活，让你充分利用投入的每一分钟"

你将能够适当地应对所有类型的网络安全威胁。注册并成为一名出色的专家。

按照自己的进度学习，不受干扰，没有死板的时间表：TECH 的教学方法就是这么方便。

该课程的教学人员包括该行业的专业人士，他们将自己的工作经验注入到培训中。

其多媒体内容采用最新教育科技开发，将使专业人员在情景式学习环境中学习，即模拟环境，提供身临其境的培训程序，在真实情况下进行培训。

该方案的设计重点是基于问题的学习，通过这种学习，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。它将得到一个由著名专家开发的创新互动视频系统的支持。

02

目标

考虑到网络安全领域的复杂性与日俱增，本信息科技安全管理专科文凭的主要目标是让专业人员更接近该领域最重要的发展。通过这种方式，你将成为该领域的优秀专家，能够管理和指导各行各业公司的网络安全工作。

通过该课程，TECH帮助你申请最重要的
国内和国际公司的重要专业职位"

总体目标

- 开发一个信息安全管理系统(ISMS)
- 识别构成ISMS的关键因素
- 评估安全架构的不同模式,以建立最适合组织的模式
- 辨识应用的监管框架及其监管基础
- 分析一个信息安全领域(CISO办公室)的组织和职能结构
- 建立一个审计方案,涵盖组织在网络安全的自我评估需求
- 制定一个漏洞扫描和监测方案以及网络安全事件应对计划
- 以 ISO-22301 指南为基础,确定业务连续性计划 (BCP) 的基本要素
- 审查未制定业务连续性计划 (BCP) 所带来的风险
- 分析业连计划的成功标准及其与公司整体风险管理的结合
- 明确业务连续性计划的实施阶段

具体目标

模块1.信息安全架构和模式

- 使总体安全计划与组织的战略目标保持一致
- 建立一个持续的风险管理框架，作为安全总计划的一个组成部分
- 确定适当的指标来监测ISMS的实施情况
- 建立一个基于政策的安全战略
- 分析与员工、供应商和合作伙伴计划的目标和程序
- 在监管框架内，确定适用于每个组织的法规、认证和法律
- 制定ISO 27001:2013标准要求的基本要素
- 实施符合欧洲GDPR/RGPD法规的隐私管理模式

模块2.IT安全管理

- 识别一个信息安全领域可能具有的不同结构
- 制定一个基于三道防线的安全模型
- 介绍网络安全领域参与的各种定期和特别委员会
- 规定支持安全运营团队（SOC）主要功能的技术工具
- 评估适合于每种情况的脆弱性控制措施
- 在NIST CSF的基础上制定安全操作框架
- 明确不同类型审计的范围（红队审计、五项测试、漏洞赏金审计，等）
- 提出安全事件发生后应开展的活动
- 建立一个包括所有相关行为者（当局、客户、供应商等）的信息安全指挥中心

模块3.与安全有关的业务连续性计划

- 介绍每个阶段的关键要素，分析业务连续性计划（BCP）的特点
- 证明业务连续性计划的必要性
- 确定业务连续性计划的每个阶段的成功和风险图
- 具体说明如何制定实施的行动计划
- 评估业务连续性计划（BCP）的完整性
- 为你的企业成功实施业务连续性计划制定一个计划

> 你将成为所在环境中最重要的 IT 安全专家。不要再等了:现在就报名"

03

课程管理

拥有世界领先的 IT 安全管理专家，对专业人士来说是一个绝佳的机会。这正是这个专科文凭 所能提供的，由著名工程师和计算机科学家组成的师资队伍将为学生提供最先进的技术和程序，以确保公司内部的充分安全。

你将接触到一流的网络安全专家，他们将为你提供在该领域最高水平工作的所有关键"

管理人员

Olalla Bonal, Martín先生

- IBM的客户区块链的技术专家
- 区块链架构师
- 银行业基础架构架构师
- 项目管理和解决方案的启动
- 数码电子技术员
- 教学人员公司的 Hyperledger Fabric 培训
- 教学人员公司业务的区块链培训

教师

Gozalo Fernández, Juan Luis先生

- 计算机工程师
- UNIR DevOps 和区块链的副教授
- Alastria 区块链 DevOps 的前总监
- Tinkerlink 移动应用开发总监 Cronos Telecom
- Banco Santander 的 IT 总监
- 西班牙巴克莱银行 IT 服务管理技术总监
- 国立远程教育大学 (UNED) 高等计算机工程学士

Embid Ruiz, Mario先生

- ICT法律和数据保护的律师专家
- Branddocs, SL, 可信解决方案技术公司的法务经理
- 雷伊胡安卡洛斯大学法律和工商管理学士
- Villanueva y Cremades & Calvo Sotelo 大学研究中心的新技术、互联网和视听法硕士

Rodrigo Estébanez, Juan Manuel先生

- ISMET TECH S.L.创始人
- 巴利亚多利德大学工程学位
- CFE-CEU 掌握综合管理系统
- ISO 27001 首席审核员 (IMQ)
- ISO 27001 首席实施者 (IMQ)
- 北约标准 HPS (NATO)

04

结构和内容

本信息科技安全管理专科文凭的教学大纲分为 3 个模块，学习时间为 450 个小时。在此期间，专业人员将深入研究该领域的相关方面，如取证分析、信息安全模型、适用于该领域的监管框架或网络安全规则的配置，以及其他许多问题。

你将拥有最完整的教学大纲，并可通过教学资源 24 小时随时查阅"

模块1.信息安全架构和模式

1.1. 信息安全架构
- 1.1.1. SGSI/PDS
- 1.1.2. 战略调整
- 1.1.3. 风险管理
- 1.1.4. 绩效衡量

1.2. 信息安全模型
- 1.2.1. 基于安全策略
- 1.2.2. 基于保护工具
- 1.2.3. 基于工作团队

1.3. 安全模型关键零件
- 1.3.1. 风险识别
- 1.3.2. 控制的定义
- 1.3.3. 持续评估风险水平
- 1.3.4. 员工、供应商、合作伙伴等的意识计划

1.4. 风险管理流程
- 1.4.1. 资产识别
- 1.4.2. 威胁识别
- 1.4.3. 风险评估
- 1.4.4. 控制的优先级
- 1.4.5. 重新评估和剩余风险

1.5. 业务流程和信息安全
- 1.5.1. 业务流程
- 1.5.2. 基于业务参数的风险评估
- 1.5.3. 业务影响分析
- 1.5.4. 业务运营和信息安全

1.6. 持续改进过程
- 1.6.1. 戴明循环
  - 1.6.1.1. 计划
  - 1.6.1.2. 做
  - 1.6.1.3. 核实
  - 1.6.1.4. 行动

1.7. 安全架构
- 1.7.1 技术的选择和标准化
- 1.7.2 身份管理验证
- 1.7.3 访问管理授权
- 1.7.4 网络基础设施安全
- 1.7.5 加密技术和解决方案
- 1.7.6 终端设备安全 (EDR)

1.8. 监管框架
- 1.8.1 行业法规
- 1.8.2 认证
- 1.8.3 立法

1.9. ISO 27001 标准
- 1.9.1 执行
- 1.9.2 认证
- 1.9.3 审计和渗透测试
- 1.9.4 持续风险管理
- 1.9.5 信息分类

1:10. 隐私的立法RGPD (GDPR)
- 1.10.1. 通用数据保护条例 (RGPD) 的范围
- 1.10.2. 个人资料
- 1.10.3. 个人数据处理的角色
- 1.10.4. ARCO 权利
- 1.10.5. DPO功能

模块2.IT安全管理

2.1. 安全管理
- 2.1.1. 安全行动
- 2.1.2. 法律和监管方面
- 2.1.3. 业务赋能
- 2.1.4. 风险管理
- 2.1.5. 身份和访问管理

2.2. 安全区域的结构首席信息安全官办公室
- 2.2.1. 组织结构CISO 结构的位置
- 2.2.2. 防线
- 2.2.3. CISO办公室组织结构图
- 2.2.4. 预算管理

2.3. 安全政府
- 2.3.1. 安全委员会
- 2.3.2. 风险监察委员会
- 2.3.3. 审计委员会
- 2.3.4. 危机委员会

2.4. 安全政府功能
- 2.4.1. 政策和标准
- 2.4.2. 安全总计划
- 2.4.3. 仪表板
- 2.4.4. 意识和培训
- 2.4.5. 供应链的安全

2.5. 安全行动
- 2.5.1. 身份和访问管理
- 2.5.2. 网络安全规则的配置防火墙
- 2.5.3. IDS/IPS 平台管理
- 2.5.4 漏洞扫描

2.6. 网络安全框架NIST CSF
- 2.6.1 NIST方法学
  - 2.6.1.1. 识别
  - 2.6.1.2. 保护
  - 2.6.1.3. 探测
  - 2.6.1.4. 回复
  - 2.6.1.5. 恢复

2.7. 安全运营中心 (SOC)功能
- 2.7.1. 保护红队、渗透测试、威胁情报
- 2.7.2. 检测。SIEM, 用户行为分析、欺诈预防
- 2.7.3. 答案

2.8. 安全审计
- 2.8.1. 渗透测试
- 2.8.2. 红队练习
- 2.8.3. 源代码审计安全发展
- 2.8.4. 组件安全 (软件供应链)
- 2.8.5. 取证分析

2.9. 事件响应
- 2.9.1. 准备工作
- 2.9.2. 检测、分析和通知
- 2.9.3. 遏制、根除和恢复
- 2.9.4. 事后活动
  - 2.9.4.1. 证据保留
  - 2.9.4.2. 取证分析
  - 2.9.4.3. 差距管理
- 2.9.5 官方网络事件管理指南

2:10. 漏洞管理
- 2.10.1. 漏洞扫描
- 2.10.2. 漏洞评估
- 2.10.3. 系统硬化
- 2.10.4. 第 0 天漏洞零日

模块3.与安全有关的业务连续性计划

3.1. 业务连续性计划
- 3.1.1. 业务连续性计划 (BCP)
- 3.1.2. 业务连续性计划 (BCP)关键问题
- 3.1.3. 用于公司估值的业务连续性计划 (BCP)

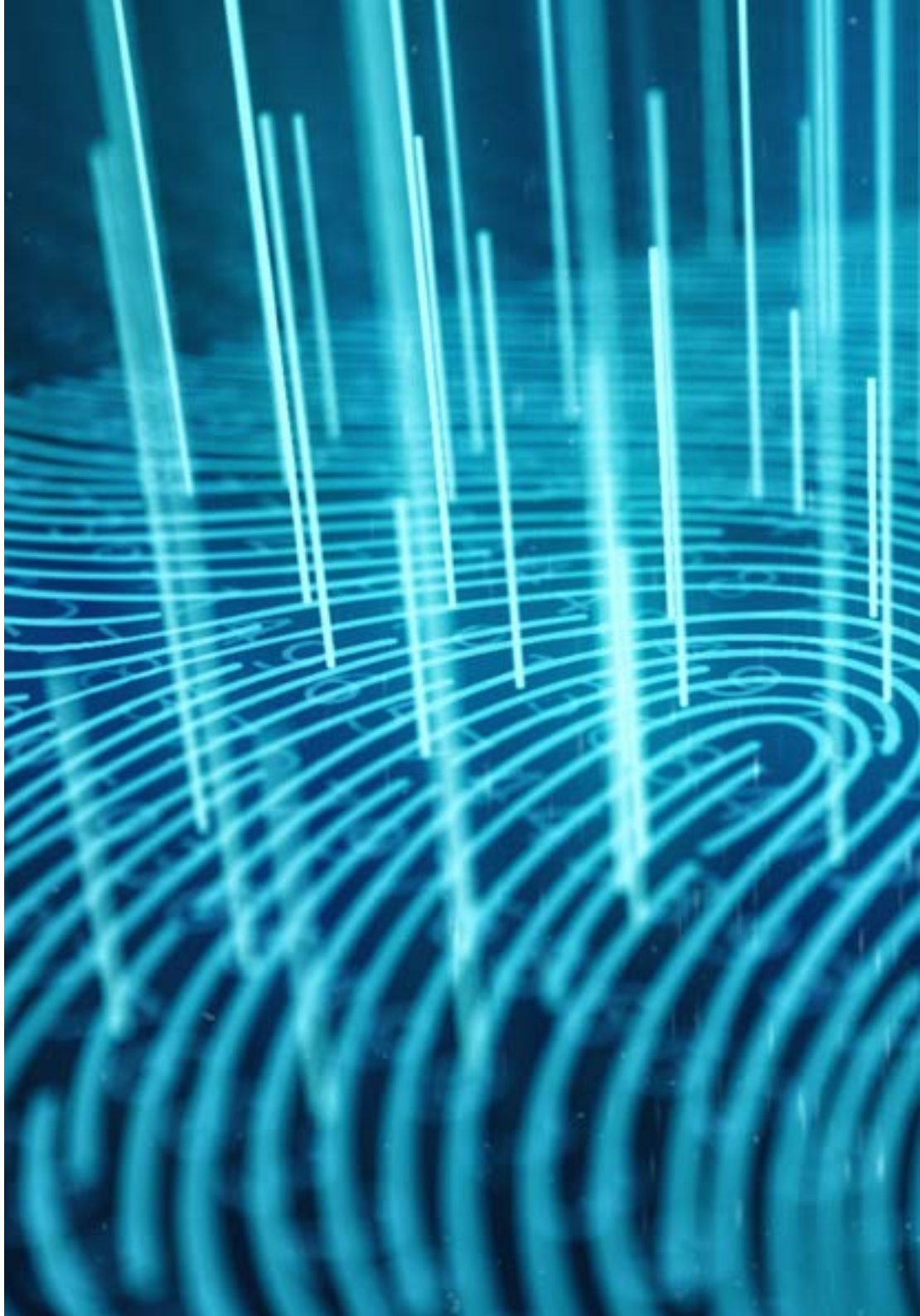
3.2. 业务连续性计划 (BCP) 中的指标
- 3.2.1. 恢复时间目标 (RTO) 和恢复点目标 (RPO)
- 3.2.2. 最大容许时间 (MTD)
- 3.2.3. 最低恢复水平 (ROL)
- 3.2.4. 恢复点目标 (RPO)

3.3. 连续性项目类型
- 3.3.1. 业务连续性计划 (BCP)
- 3.3.2. ICT 连续性计划 (PCTIC)
- 3.3.3. 灾难恢复计划(PRD)

3.4. 与 PCN 相关的风险管理
- 3.4.1. 业务影响分析
- 3.4.2. 实施 PCN 的好处
- 3.4.3. 基于风险的心态

3.5. 业务连续性计划的生命周期
- 3.5.1. 阶段1:组织分析
- 3.5.2. 阶段2 :确定连续性策略
- 3.5.3. 阶段3:应对突发事件
- 3.5.4. 阶段4:测试、维护和审查

3.6. 国家联络点组织的分析阶段
- 3.6.1. 识别 BCP 范围内的流程
- 3.6.2. 确定关键业务领域
- 3.6.3. 识别区域和流程之间的依赖关系
- 3.6.4. 确定合适的最佳可行技术
- 3.6.5. 可交付的成果创建项目



3.7. PCN中连续性策略的确定阶段
- 3.7.1. 战略确定阶段的角色
- 3.7.2. 战略确定阶段的任务
- 3.7.3. 可交付的成果

3.8. PCN 中的应急响应阶段
- 3.8.1. 响应阶段的角色
- 3.8.2. 这个阶段的任务
- 3.8.3. 可交付的成果

3.9. PCN 的测试、维护和审查阶段
- 3.9.1. 测试、维护和审查阶段的角色
- 3.9.2. 测试、维护和审查阶段的任务
- 3.9.3. 可交付的成果

3:10. 与业务连续性计划 (BCP) 相关的 ISO 标准
- 3.10.1. ISO 22301:2019
- 3.10.2. ISO 22313:2020
- 3.10.3. 其他 ISO 和国际标准

> 该计划将使你能够深入研究各种问题，如确定领域和流程之间的依赖关系，这是建立正确的网络安全的一个基本方面"

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

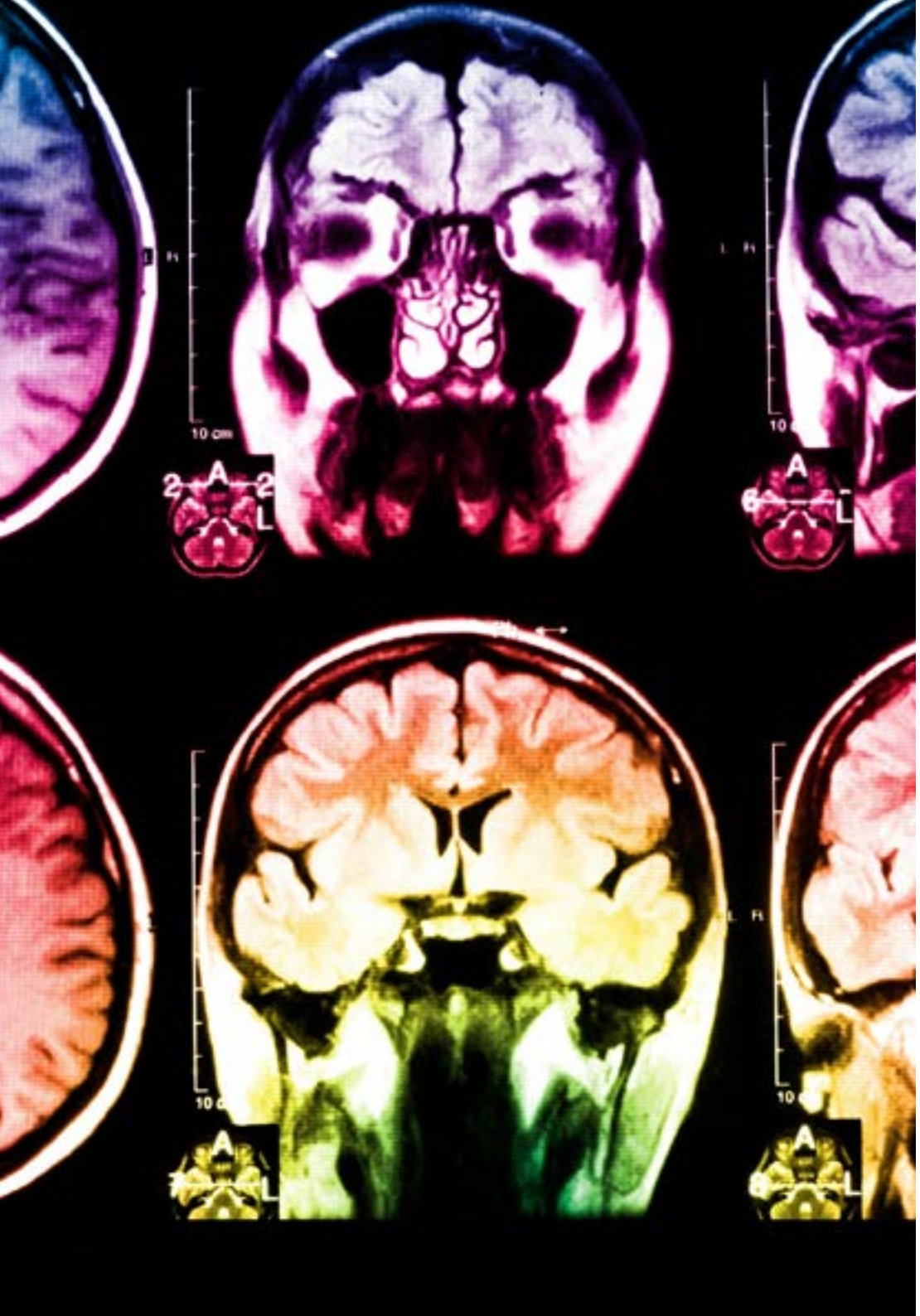
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

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。

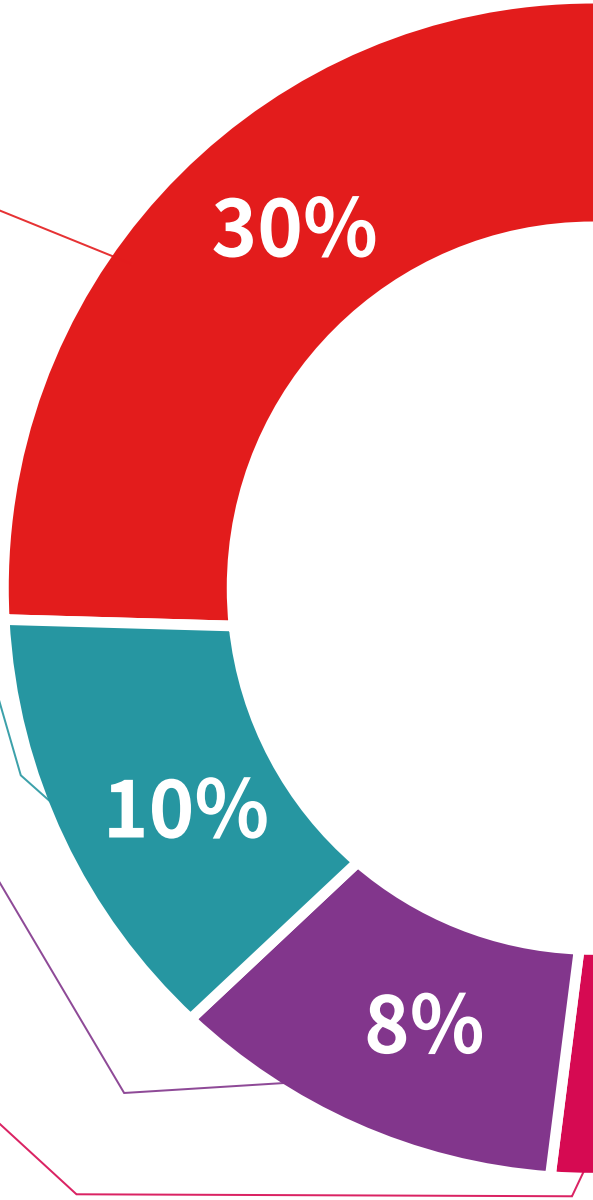
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

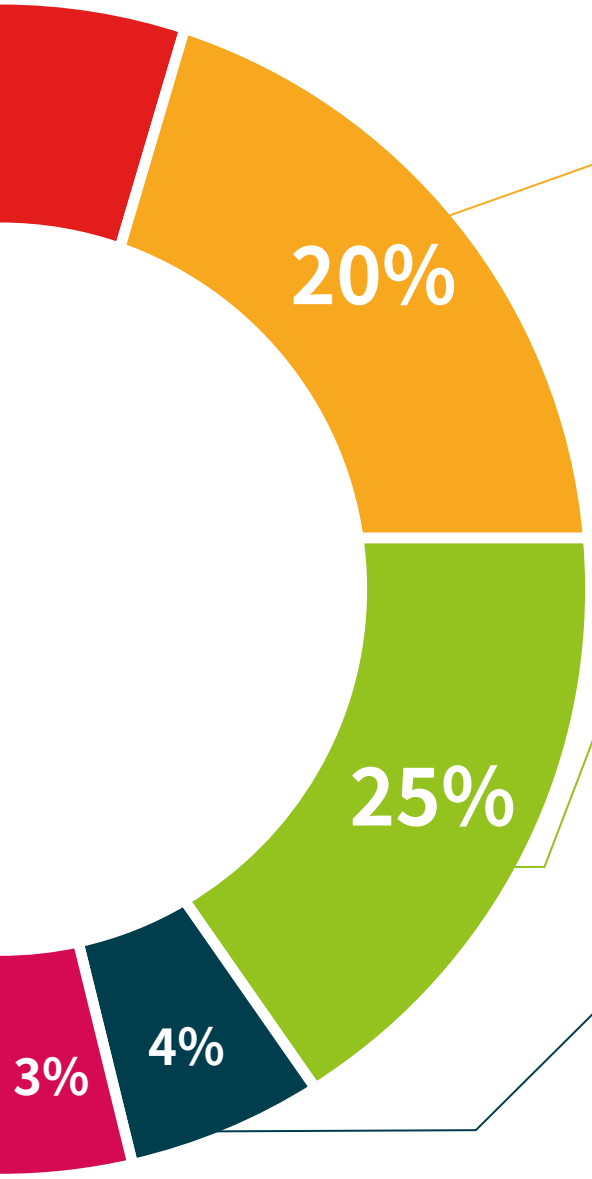
技能和能力的实践

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

信息科技安全管理专科文凭除了保证最严格和最新的培训外，还可以获得由TECH科技大学颁发的专科文凭学位证书。

成功地完成这一项目，并获得你的大学学位，没有旅行或行政文书的麻烦"

这个 **信息科技安全管理专科文凭**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**专科文凭**学位。

TECH科技大学颁发的证书将表达在专科文凭获得的资格，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：**信息科技安全管理专科文凭**

官方学时：**450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

专科文凭

信息科技安全管理

这是一个由本大学授予的学位，相当于450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

专科文凭
信息科技安全管理

- 模式:在线
- 时间:6个月
- 学历:TECH科技大学
- 时间:16小时/周
- 时间表:按你方便的
- 考试:在线

专科文凭
信息科技安全管理

tech 科学技术大学