校级硕士
在企业中网络安全政策管理

tech 科学技术大学

tech 科学技术大学

校级硕士
在企业中网络安全政策管理

- 模式:**在线**
- 时间:**12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/professional-master-degree/master-corporate-cybersecurity-policy-management

目录

01

介绍

许多企业和行业对虚拟环境的依赖性增加，反过来又导致了网络犯罪和对所有类型组织的网络攻击的扩散。无论规模或地点如何，网络安全威胁构成了真正的危险，可能导致时间,金钱和数据的大量损失。出于这个原因，具有网络安全政策管理具体知识的计算机科学家的身影在商业领域变得越来越重要，在职业和个人发展方面都有大量的机会。这个学位为IT专业人士提供了一个无与伦比的机会，让他们的职业生涯得到推动，并得到一个在该领域具有丰富经验的专业团队的支持。100%在线的学位形式也使其成为与各种活动或责任完全兼容的选择。

现在注册，就可以获得关于事件管理政策，软件和硬件安全以及实用安全灾难恢复的专门内容”

每天都有数以千计的网络犯罪分子攻击世界各地的公司，甚至在数千公里之外，这使得网络安全成为现代商业领域的主要关切。依靠虚拟环境的组织中的漏洞可能被各种犯罪分子利用，窃取敏感数据或阻止其访问以换取赎金。

这就是为什么正确管理公司的网络安全政策需要一个巨大的责任，因为这个责任位置对专业的IT专家来说是一个很高的声誉和经济预测。因此，抓住机会，深入研究审计系统定位威胁或安全通信协议等主题，是对任何组织中的关键职位的直接提升。

对于这个校级硕士，由TECH精心挑选的一批教师已经准备了一流的教学内容。通过10个综合模块，计算机科学家将扩大他们在实施物理和环境安全政策,信息安全管理系统,监测工具和许多其他技能方面的技能，使他们成为任何机构的宝贵资产。

所有这些都具有不可否认的优势，即不必参加面对面的课程或固定的时间表，因为整个课程都是在线教学。教学内容可以从任何有互联网连接的设备上下载，甚至可以在完成学位后作为参考指南使用。计算机科学家将有根据自己的节奏调整课程量的自由，能够将其与他们通常的专业活动或更苛刻的责任相结合。

这个**在企业中网络安全政策管理校级硕士**包含了市场上最完整和最新的课程。主要特点是：

- 由IT网络安全专家介绍案例研究的发展情况
- 本书的内容图文并茂,示意性强,实用性强，为那些专业实践中必不可少的学科提供技术和实用信息
- 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

> 将自己定位为一名有偿网络安全政策官员，适应IT安全领域的各种情况和突发事件”

> 将最有效的攻击安全政策实践纳入你的日常工作，并由该领域的专家团队加以完善”

进入一个多媒体丰富的教学大纲，通过管理安全政策,IT风险分类和劫持的具体主题来加强。

你将能够选择何时,何地和如何承担全部课程，完全自由地按照自己的进度完成教学大纲。

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。

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。

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。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

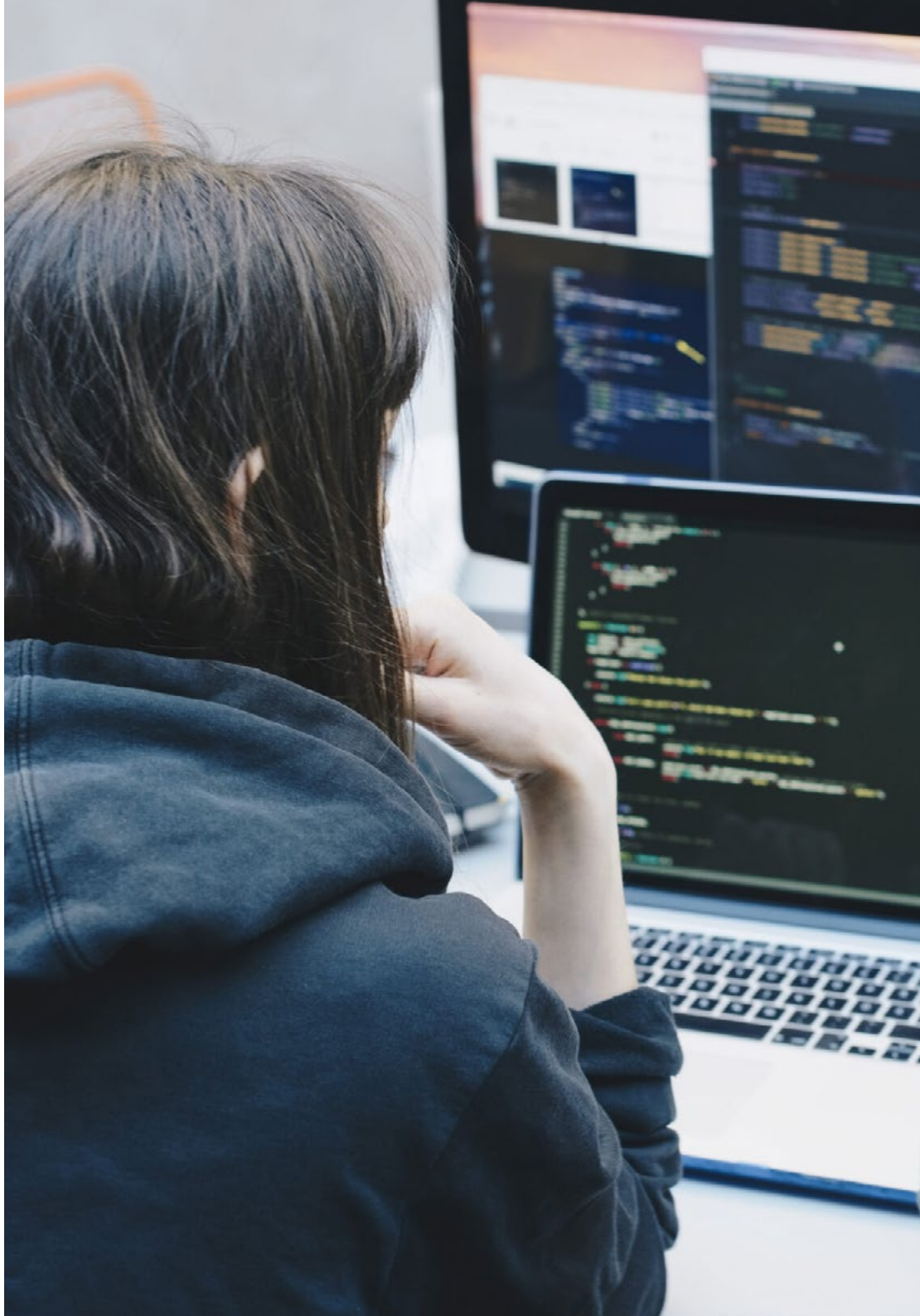
由于网络安全是当今商业世界的一个重要问题，这个学位将计算机科学家的角色作为处理这些问题的核心部分。出于这个原因，整个教学大纲所追求的目标是多样化的，优先提供基于计算机安全最新进展的最新理论内容。

你将拥有一份关于网络安全政策管理的参考指南，它将帮助你提升你作为数字安全IT专家的职业生涯”

总体目标

- 加深对信息安全关键概念的理解
- 制定必要的措施以确保良好的信息安全做法
- 制定不同的方法来进行详尽的威胁分析
- 安装和学习用于治疗和预防事故的不同工具

> TECH的教学方法将使你甚至比你预期的更快地实现你最雄心勃勃的目标”



具体目标

模块1.信息安全管理系统(ISMS)
- 分析目前适用于ISMS的法规和标准
- 制定在一个实体中实施ISMS的必要阶段
- 分析信息安全事件管理和实施程序

模块2.信息安全政策的组织方面
- 在公司实施ISMS
- 确定安全管理系统的实施应涵盖哪些部门
- 在行动中实施必要的安全对策

模块3.IT系统中威胁分析的安全政策
- 分析威胁的含义
- 确定预防性威胁管理的阶段
- 比较不同的威胁管理方法

模块4.软件和硬件中安全策略的实际实施
- 确定什么是认证和识别
- 分析现有的不同认证方法及其实际执行情况
- 为软件和系统实施正确的访问控制政策
- 建立当前主要的识别技术
- 产生关于系统堡垒化的不同方法的专门知识

模块5.安全事件管理政策
- 发展关于如何管理计算机安全事件引起的事件的专业知识
- 确定安全事件处理小组的运作方式
- 分析IT安全事件管理的不同阶段
- 审查处理安全事件的标准化协议安全事件

模块6.在公司实施实体和环境安全政策
- 分析安全区和安全周界这一术语
- 考察生物识别技术和生物识别系统
- 实施正确的安全政策以保障实体安全
- 制定关于计算机系统安全领域的现行法规

模块7.企业中的安全通信政策
- 通过划分网络确保通信网络的安全
- 分析通信网络中使用的不同加密算法
- 在网络中实施各种加密技术，如TLS,VPN或SSH

模块8.面对攻击时安全政策的实际执行情况
- 确定对我们信息系统的不同实际攻击
- 评估不同的安全策略以减轻攻击的影响
- 从技术上采取措施，减轻主要威胁

模块9.信息系统安全政策中的监测工具
- 发展监测和衡量标准实施的概念
- 在系统上配置审计跟踪并监控网络
- 汇编目前市场上最好的系统监控工具

模块10.实用的安全灾难恢复政策
- 生成关于信息安全连续性概念的专门知识
- 制定一个业务连续性计划
- 分析一个业务连续性计划
- 设计一个灾难恢复计划

03

能力

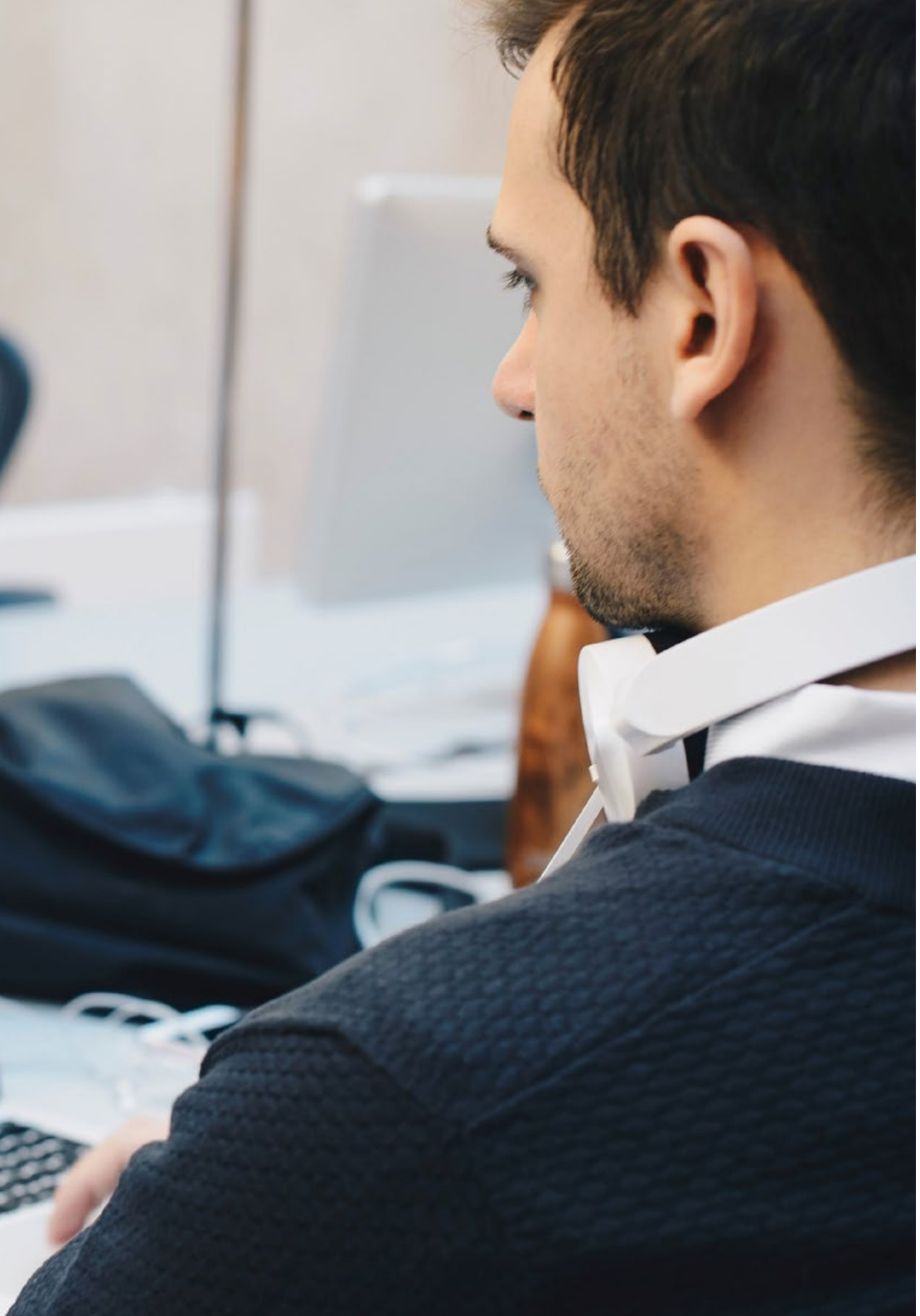
为了培养网络安全政策方面的IT专家所必须具备的先进和专业技能，TECH已经吸收了一批优秀的教学人员。通过专业经验和数字安全的最新发展的实际结合，计算机科学家将获得所涵盖的每个主题的更大背景，并有广泛的例子和多媒体资源来支持。

你将获得一套技能，突出你在组织的任何网络战略计划中的关键重要性”

总体能力

- 根据每种类型的实体及其需要，实施和制定业务连续性计划
- 制定业务流程分析
- 分析审计方法
- 评估对计算机取证分析的需求，以深入研究记录的事件

> 由于网络安全的专业性，你将能够提高你的工作和工资预测，这是目前最受关注的主题”



具体能力

- 确定ISMS在实体的内部组织中的参与度，以及它的地位
- 建立公司的安全政策
- 确定我们需要对供应商和信息系统的维护实施哪些措施
- 产生关于威胁控制的专门知识
- 确定预防性威胁管理的阶段
- 制定IT威胁分析的方法
- 按影响和严重程度对威胁进行分类
- 设计你自己的预防性威胁分析和控制的方法
- 对网络和服务实施正确的访问控制政策
- 分析正确处理安全事件的重要性安全事件
- 汇编现有的不同生物识别系统
- 考察生物识别技术和生物识别系统
- 在数据中心实施正确的物理安全政策和物理访问控制系统
- 实施一个安全的网络
- 检查移动和物联网平台的漏洞以及如何避免这些漏洞
- 建立社会工程的类型，并学习如何减轻它们的影响
- 分析监测和衡量标准实施的概念
- 确定对信息安全连续性的需求

04

课程管理

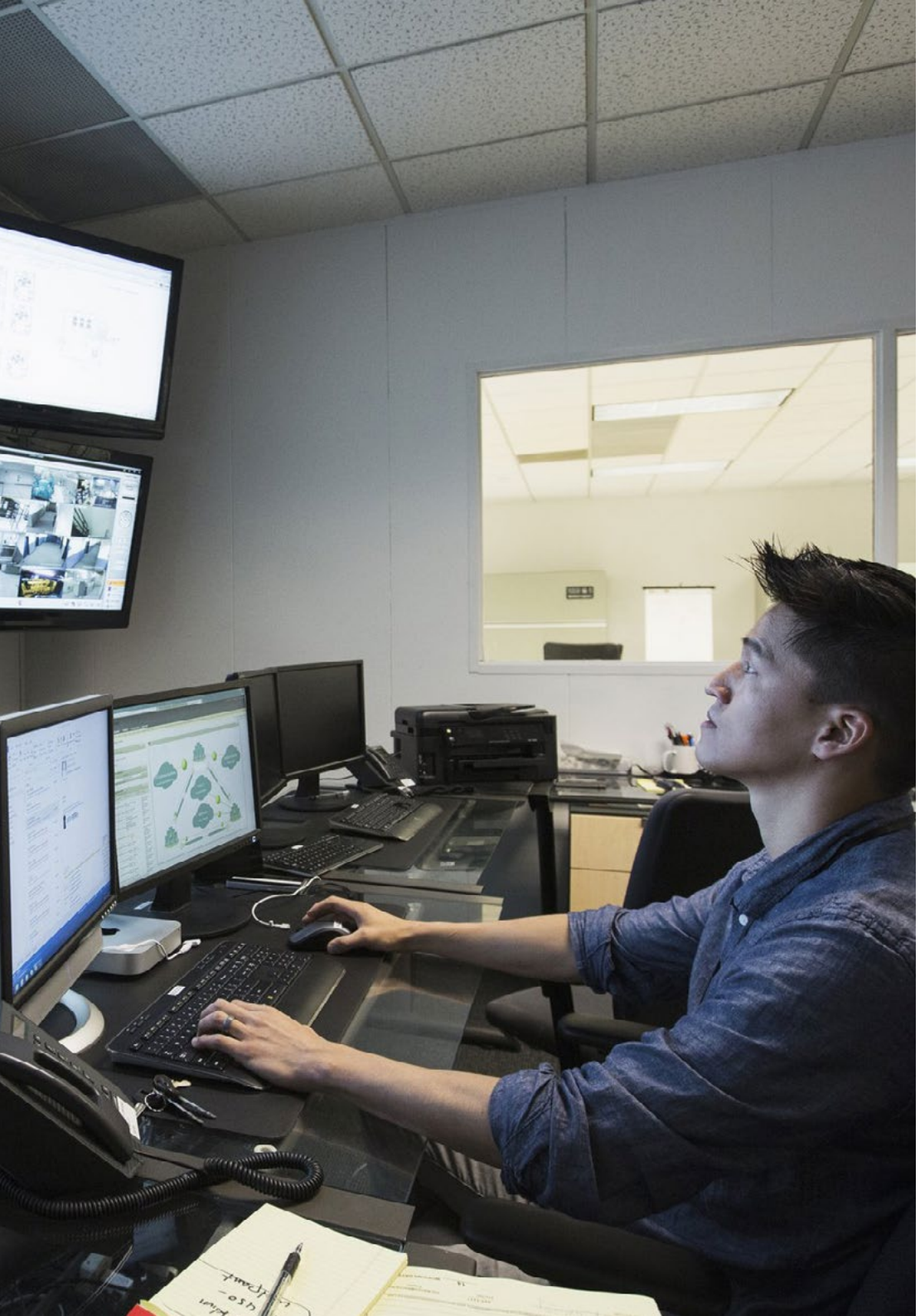
TECH为这个校级硕士选择的所有专业人员都在IT服务管理领域有丰富的经验，始终关注网络安全和协议的正确执行。准确地说，正是这种经验使整个教学大纲具有更高的质量，因为其突出的实用性，使得计算机科学家可以立即采用所有的新知识，甚至在完成学位之前就提高他们的技能。

你将得到一个教学团队的支持和帮助，致力于最大限度地提高你在网络安全政策管理方面的专业水平”

管理人员

Fernández Sapena, Sonia 女士

- 巴利阿里群岛大学的首席安全官
- 不同大学的高级安全架构师
- 苏菲和UIB的Campus Extens的IT安全主管
- 毕业于阿尔卡拉德埃纳雷斯大学的计算机工程专业
- DevOps领域的大师。网络商业中心的Docker和Kubernetes



教师

Oropesiano Carrizosa, Francisco 先生

- 网络服务经理/邮件/DNS/内容管理系统经理
- 网络和服务器系统安全技术员
- 网站设计和制作
- 毕业于阿尔卡拉德埃纳雷斯大学医学和外科专业
- DevOps领域的大师。网络商业中心的Docker和Kubernetes
- 网络和电信专业的校级硕士

Peralta Alonso, Jon 先生

- Altia Consultores S.A.的律师/DPO
- Arriaga Asociados Asesoramiento Jurídico y Económico, S.L. 的律师/法律顾问
- Kutxabank的商务经理
- 毕业于巴斯克地区公立大学法律专业
- EIS创新学校的数据保护硕士代表
- 在巴斯克地区公立大学获得法学校级硕士

Ortega López, Florencio 先生

- 私营和上市公司的ICT和安全顾问
- 毕业于阿尔卡拉德埃纳雷斯大学医学和外科专业
- 大学教职员工的校级硕士证书
- 在IDE-CESEM学习管理和商业管理的MBA课程
- IDE-CESEM的管理和信息技术管理校级硕士

05

结构和内容

TECH采用的方法是 再学习 以制定本方案的所有内容。这意味着网络安全政策管理中最重要的关键概念将在整个教学大纲中逐步给出，从而使教学更加有效和快速。计算机科学家将有机会接触到许多详细的视频,自我意识练习和专门为该方案的每个主题选择的补充读物。

这个校级硕士中包含的所有多媒体材料将帮助你以更深,更快,更详尽的方式进行专业学习”

模块1.信息安全管理制度

1.1. 信息的安全问题。关键问题
- 1.1.1. 信息的安全问题
  - 1.1.1.1. 保密性
  - 1.1.1.2. 整合
  - 1.1.1.3. 可提供的服务
  - 1.1.1.4. 信息安全措施

1.2. 信息安全管理制度
- 1.2.1. 信息安全管理模型
- 1.2.2. 实施ISMS的文件
- 1.2.3. ISMS的级别和控制

1.3. 国际规范和标准
- 1.3.1. 信息安全方面的国际标准
- 1.3.2. 标准的起源和演变
- 1.3.3. 国际信息安全管理标准
- 1.3.4. 其他参考标准

1.4. ISO/IEC 27.000标准
- 1.4.1. 目的和范围
- 1.4.2. 标准的结构
- 1.4.3. 认证
- 1.4.4. 认证的各个阶段
- 1.4.5. ISO/IEC 27.000标准的好处

1.5. 设计和实施一个整体的信息安全系统
- 1.5.1. 设计和实施一个整体的信息安全系统
- 1.5.2. 一般信息安全系统的实施阶段
- 1.5.3. 业务连续性计划

1.6. 第一阶段：诊断
- 1.6.1. 初步诊断
- 1.6.2. 确定分层的水平
- 1.6.3. 对标准/规范的遵守程度

1.7. 第二阶段：准备
- 1.7.1. 组织背景
- 1.7.2. 对适用的安全法规的分析
- 1.7.3. 一般信息安全系统的范围
- 1.7.4. 一般信息安全系统的政策
- 1.7.5. 一般信息安全系统的目标

1.8. 第三阶段：规划
- 1.8.1. 资产的分类
- 1.8.2. 风险评估
- 1.8.3. 识别威胁和风险

1.9. 第四阶段：实施和监测
- 1.9.1. 结果分析
- 1.9.2. 分配责任
- 1.9.3. 行动计划的时间安排
- 1.9.4. 监测和审计

1.10. 事故管理安全政策
- 1.10.1. 阶段
- 1.10.2. 事件的分类
- 1.10.3. 事故程序和事故管理

模块2.信息安全政策的组织方面

2.1. 内部组织
- 2.1.1. 分配责任
- 2.1.2. 职责分离
- 2.1.3. 与当局的联系
- 2.1.4. 项目管理中的信息安全

2.2. 资产管理
- 2.2.1. 对资产的责任
- 2.2.2. 信息的分类问题
- 2.2.3. 存储介质的处理

2.3. 业务流程中的安全政策
- 2.3.1. 对脆弱的业务流程进行分析
- 2.3.2. 业务影响分析
- 2.3.3. 根据业务影响对流程进行排序

2.4. 与人力资源部门相关的安全政策
- 2.4.1. 聘用前
- 2.4.2. 招聘期间
- 2.4.3. 终止或改变职位

2.5. 管理安全政策
- 2.5.1. 信息安全管理准则
- 2.5.2. BIA - 分析影响
- 2.5.3. 作为安全政策的恢复计划

2.6. 信息系统的获取和维护
- 2.6.1. 信息系统安全要求
- 2.6.2. 开发和支持数据安全
- 2.6.3. 测试数据

2.7. 与供应商的安全关系
- 2.7.1. 供应商的IT安全
- 2.7.2. 提供有保障的服务的管理
- 2.7.3. 供应链安全

2.8. 业务安全
- 2.8.1. 业务责任
- 2.8.2. 对恶意代码的保护
- 2.8.3. 后备副本
- 2.8.4. 活动日志和监测

2.9. 安全管理和法规
- 2.9.1. 安全管理和法规
- 2.9.2. 遵守法律规定
- 2.9.3. 信息安全审查

2.10. 业务连续性管理中的安全问题
- 2.10.1. 业务连续性管理中的安全问题
- 2.10.2. 信息安全的延续性
- 2.10.3. 裁员

模块3.信息系统的安全政策 威胁分析

3.1. 安全政策中的威胁管理
- 3.1.1. 安全政策中的威胁管理
- 3.1.2. 安全风险
- 3.1.3. 威胁管理的方法
- 3.1.4. 方法的实施

3.2. 威胁管理的各个阶段
- 3.2.1. 鉴定
- 3.2.2. 分析报告
- 3.2.3. 地点
- 3.2.4. 保障措施

3.3. 威胁定位的审计系统
- 3.3.1. 威胁定位的审计系统
- 3.3.2. 分类和信息流
- 3.3.3. 对脆弱流程进行分析

3.4. 风险分类
- 3.4.1. 风险的类型
- 3.4.2. 危险概率的计算
- 3.4.3. 剩余风险

3.5. 风险处理
- 3.5.1. 风险处理
- 3.5.2. 保障措施的实施
- 3.5.3. 转让或承担

3.6. 风险控制
- 3.6.1. 持续的风险管理过程
- 3.6.2. 安全指标的实施
- 3.6.3. 信息安全度量的战略模式

3.7. 信息安全度量的战略模式
- 3.7.1. 威胁目录
- 3.7.2. 控制措施目录
- 3.7.3. 保障措施目录

3.8. ISO 27005
- 3.8.1. 风险识别
- 3.8.2. 风险分析
- 3.8.3. 风险评估

3.9. 风险,影响和威胁矩阵
- 3.9.1. 数据,系统和人员
- 3.9.2. 威胁概率
- 3.9.3. 损害的程度

3.10. 危害分析中的阶段和过程设计
- 3.10.1. 确定组织的关键因素
- 3.10.2. 威胁和影响的确定
- 3.10.3. 影响和风险分析
- 3.10.4. 方法

模块4.实际执行软件和硬件安全政策

4.1. 实际执行软件和硬件安全政策
- 4.1.1. 实施识别和授权
- 4.1.2. 实施识别技术
- 4.1.3. 授权的技术措施

4.2. 识别和授权技术
- 4.2.1. 识别码和OTP
- 4.2.2. Token USB 或PKI智能卡
- 4.2.3. ”保密辩护 ”键
- 4.2.4. 有源RFID

4.3. 软件和系统访问安全政策
- 4.3.1. 实施访问控制政策
- 4.3.2. 实施通信访问政策
- 4.3.3. 访问控制的安全工具类型

4.4. 用户访问管理
- 4.4.1. 访问权限管理
- 4.4.2. 访问角色和功能的分离
- 4.4.3. 系统中访问权限的实施

4.5. 控制对系统和应用程序的访问
- 4.5.1. 最低准入规则
- 4.5.2. 安全登录技术
- 4.5.3. 密码安全政策

4.6. 识别系统技术
- 4.6.1. 活动目录
- 4.6.2. OTP
- 4.6.3. PAP, CHAP
- 4.6.4. KERBEROS, DIAMETER, NTLM

4.7. 系统堡垒化的CIS控制
- 4.7.1. 基本的CIS控制
- 4.7.2. 基础的CIS控制
- 4.7.3. 组织上的CIS控制

4.8. 业务安全
- 4.8.1. 对恶意代码的保护
- 4.8.2. 后备副本
- 4.8.3. 记录活动和监测

4.9. 技术漏洞的管理
- 4.9.1. 技术漏洞
- 4.9.2. 技术漏洞的管理
- 4.9.3. 软件安装的限制

4.10. 安全政策实践的实施
- 4.10.1. 安全政策实践的实施
- 4.10.2. 逻辑上的漏洞
- 4.10.3. 国防政策的实施

模块5.安全事件管理政策

5.1. 信息安全事件管理政策和改进措施
- 5.1.1. 事故管理
- 5.1.2. 责任和程序
- 5.1.3. 事件通知

5.2. 入侵检测和预防系统(IDS/IPS)
- 5.2.1. 系统运行数据
- 5.2.2. 入侵检测系统的类型
- 5.2.3. IDS/IPS的位置标准

5.3. 安全事件应对
- 5.3.1. 信息收集程序
- 5.3.2. 入侵验证过程
- 5.3.3. CERT机构

5.4. 入侵企图通知和管理过程
- 5.4.1. 通知过程中的责任
- 5.4.2. 事件的分类
- 5.4.3. 解决和恢复过程

5.5. 法医分析作为一种安全政策
- 5.5.1. 挥发性和非挥发性证据
- 5.5.2. 分析和收集电子证据
  - 5.5.2.1.分析电子证据
  - 5.5.2.2.收集电子证据

5.6. 入侵检测和预防系统(IDS/IPS)工具
- 5.6.1. Snort
- 5.6.2. Suricata
- 5.6.3. Solar-Winds

5.7. 事件集中化工具
- 5.7.1. SIM
- 5.7.2. SEM.
- 5.7.3. SIEM

5.8. CCN-STIC安全指南 817
- 5.8.1. CCN-STIC安全指南 817
- 5.8.2. 网络事件管理
- 5.8.3. 衡量标准和指标

5.9. NIST SP800-61
- 5.9.1. 计算机安全事件响应能力
- 5.9.2. 事故处理
- 5.9.3. 协调和信息共享

5.10. ISO 27035
- 5.10.1. ISO 27035事件管理的原则
- 5.10.2. 制定事故管理计划的准则
- 5.10.3. 突发事件应对行动指南

模块6.在企业中实施安全和环境安全政策

6.1. 安全区域
- 6.1.1. 物理安全周边
- 6.1.2. 在安全区域工作
- 6.1.3. 办事处,办公室和资源的安全

6.2. 实际进入控制
- 6.2.1. 实际进入控制
- 6.2.2. 物理访问控制政策
- 6.2.3. 物理入口控制系统

6.3. 物理访问漏洞
- 6.3.1. 物理访问漏洞
- 6.3.2. 主要的物理脆弱性
- 6.3.3. 保障措施的实施

6.4. 生理生物识别系统
- 6.4.1. 指纹
- 6.4.2. 面部识别
- 6.4.3. 虹膜和视网膜识别
- 6.4.4. 其他生理生物识别系统

6.5. 行为生物识别系统
- 6.5.1. 签名确认
- 6.5.2. 作家认可
- 6.5.3. 语音识别
- 6.5.4. 其他生物识别行为系统

6.6. 生物统计学的风险管理
- 6.6.1. 生物统计学的风险管理
- 6.6.2. 生物识别系统的实施
- 6.6.3. 生物识别系统的弱点

6.7. 在 hosts政策的实施
- 6.7.1. 安装布线供应和安全
- 6.7.2. 设备位置
- 6.7.3. 场所外设备的出口
- 6.7.4. 无人看管的IT设备和明确的岗位政策

6.8. 环境保护
- 6.8.1. 消防系统
- 6.8.2. 地震防护系统
- 6.8.3. 地震防护系统

6.9. 数据处理中心安全
- 6.9.1. 安全门
- 6.9.2. 视频监控系统 (CCTV)
- 6.9.3. 安全控制

6.10. 国际实体安全条例
- 6.10.1. IEC 62443-2-1 (欧规)
- 6.10.2. NERC CIP-005-5 (EEUU)
- 6.10.3. NERC CIP-014-2 (EEUU)

模块7.企业中的安全通信政策

7.1. 网络安全管理
- 7.1.1. 网络控制和监测
- 7.1.2. 网络隔离
- 7.1.3. 网络安全系统

7.2. 安全通信协议
- 7.2.1. TCP/IP模型
- 7.2.2. IPSEC 协议
- 7.2.3. TLS 协议

7.3. TLS 1.3协议
- 7.3.1. TLS1.3进程的各个阶段
- 7.3.2. 协议 Handshake
- 7.3.3. 注册协议
- 7.3.4. 与TLS 1.2的区别

7.4. 加密算法
- 7.4.1. 通信中使用的加密算法
- 7.4.2. Cipher-suites
- 7.4.3. TLS 1.3允许的加密算法

7.5. 功能 Digest
- 7.5.1. 功能 Digest
- 7.5.2. MD6
- 7.5.3. SHA

7.6. PKI. 公钥基础设施
- 7.6.1. PKI 及其实体
- 7.6.2. 数字证书
- 7.6.3. 数字证书的类型

7.7. 隧道和运输通
- 7.7.1. 隧道通信
- 7.7.2. 运输通讯
- 7.7.3. 加密隧道的实施

7.8. SSH. Secure Shell
- 7.8.1. SSH.安全胶囊
- 7.8.2. SSH的运作
- 7.8.3. SSH工具

7.9. 审计加密系统
- 7.9.1. 审计加密系统
- 7.9.2. 完整性测试
- 7.9.3. 加密系统测试

7.10. 加密系统
- 7.10.1. 加密系统
- 7.10.2. 加密系统漏洞
- 7.10.3. 密码学保障措施

模块8.面对攻击时安全政策的实际执行情况

8.1. System Hacking
- 8.1.1. System Hacking
- 8.1.2. 风险和脆弱性
- 8.1.3. 反措施

8.2. 服务中的DoS
- 8.2.1. 服务中的DoS
- 8.2.2. 风险和脆弱性
- 8.2.3. 反措施

8.3. Session Hijacking
- 8.3.1. Session Hijacking
- 8.3.2. Hijacking过程
- 8.3.3. Hijacking的反措施

8.4. Firewalls and Honeypots的规避IDS
- 8.4.1. Firewalls and Honeypots的规避IDS
- 8.4.2. 躲避技巧
- 8.4.3. 实施反措施

8.5. Hacking Web Servers
- 8.5.1. Hacking Web Servers
- 8.5.2. 对servidores webs的攻击
- 8.5.3. 实施防御措施

8.6. Hacking Web Applications
- 8.6.1. Hacking Web Applications
- 8.6.2. 对aplicaciones web的攻击
- 8.6.3. 实施防御措施

8.7. Hacking Wireless Networks
- 8.7.1. Hacking Wireless Networks
- 8.7.2. Wifi网络漏洞
- 8.7.3. 实施防御措施

8.8. Hacking Mobile Platforms
- 8.8.1. Hacking Mobile Platforms
- 8.8.2. 移动平台的弱点
- 8.8.3. 实施反措施

8.9. Ramsonware
- 8.9.1. Ramsonware
- 8.9.2. Ramsonware的导致漏洞
- 8.9.3. 实施反措施

8.10. 社会工程
- 8.10.1. 社会工程
- 8.10.2. 社会工程的类型
- 8.10.3. 社会工程的应对措施

模块9.信息系统安全政策中的监测工具

9.1. 信息系统监控政策
- 9.1.1. 系统监测
- 9.1.2. 度量衡
- 9.1.3. 衡量标准的类型

9.2. 系统审计和日志记录
- 9.2.1. 系统审计和记录
- 9.2.2. Windows审计和日志记录
- 9.2.3. 系统审计和日志记录

9.3. SNMP 协议 Simple Network Management Protocol
- 9.3.1. SNMP 协议
- 9.3.2. SNMP的运作
- 9.3.3. SNMP工具

9.4. 网络监控
- 9.4.1. 网络监控
- 9.4.2. 控制系统中的网络监控
- 9.4.3. 控制系统的监测工具

9.5. Nagios网络监控系统
- 9.5.1. Nagios
- 9.5.2. Nagios的功能
- 9.5.3. Nagios的安装

9.6. Zabbix. 网络监控系统
- 9.6.1. Zabbix
- 9.6.2. Zabbix的功能
- 9.6.3. Zabbix的安装

9.7. Cacti. 网络监控系统
- 9.7.1. Cacti
- 9.7.2. Cacti的功能
- 9.7.3. Cacti的安装

9.8. Pandora. 网络监控系统
- 9.8.1. Pandora
- 9.8.2. Pandora的功能
- 9.8.3. Pandora的安装

9.9. SolarWinds. 网络监控系统
- 9.9.1. SolarWinds
- 9.9.2. SolarWinds的功能
- 9.9.3. SolarWinds的安装

9.10. 监测条例
- 9.10.1. 监测条例
- 9.10.2. CIS对审计和记录的控制
- 9.10.3. NIST 800-123 (EEUU)

模块10.实用的安全灾难恢复政

10.1. DRP. 灾难恢复计
- 10.1.1. DRP的目的
- 10.1.2. DRP的好处
- 10.1.3. 没有PRA和没有保持更新的后果

10.2. 定义DRP（灾难恢复计划）的指南
- 10.2.1. 范围和目标
- 10.2.2. 设计恢复战略
- 10.2.3. 角色和责任的分配
- 10.2.4. 盘点hardware, software 和服务
- 10.2.5. 对停机时间和数据丢失的容忍度
- 10.2.6. 确定所需的DRP的具体类型
- 10.2.7. 实施培训,宣传和沟通计划

10.3. 灾难恢复计划（DRP）的范围和目标
- 10.3.1. 确保响应
- 10.3.2. 技术组件
- 10.3.3. 连续性政策的范围

10.4. 设计一个DRP（灾难恢复）战略
- 10.4.1. 灾难恢复战略
- 10.4.2. 预算
- 10.4.3. 人力和物力资源
- 10.4.4. 有风险的管理职位
- 10.4.5. 技术
- 10.4.6. 数据

10.5. 信息流程的连续性
- 10.5.1. 连续性规划
- 10.5.2. 连续性的实施
- 10.5.3. 核实和评价连续性

10.6. BCP（业务连续性计划）的范围
- 10.6.1. 确定最关键的过程
- 10.6.2. 基于资产的方法
- 10.6.3. 过程方法

10.7. 实施有保证的业务流程
- 10.7.1. 优先活动(PA)
- 10.7.2. 理想恢复时间（IRT）
- 10.7.3. 生存策略

10.8. 组织分析
- 10.8.1. 信息收集
- 10.8.2. 业务影响分析（BIA）
- 10.8.3. 组织风险分析

10.9. 意外处置
- 10.9.1. 危机处理计划
- 10.9.2. 业务环境恢复计划
- 10.9.3. 技术工作或事故程序

10.10. 国际标准ISO 27031 BCP
- 10.10.1. 目标
- 10.10.2. 术语和定义
- 10.10.3. 运作

06

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。

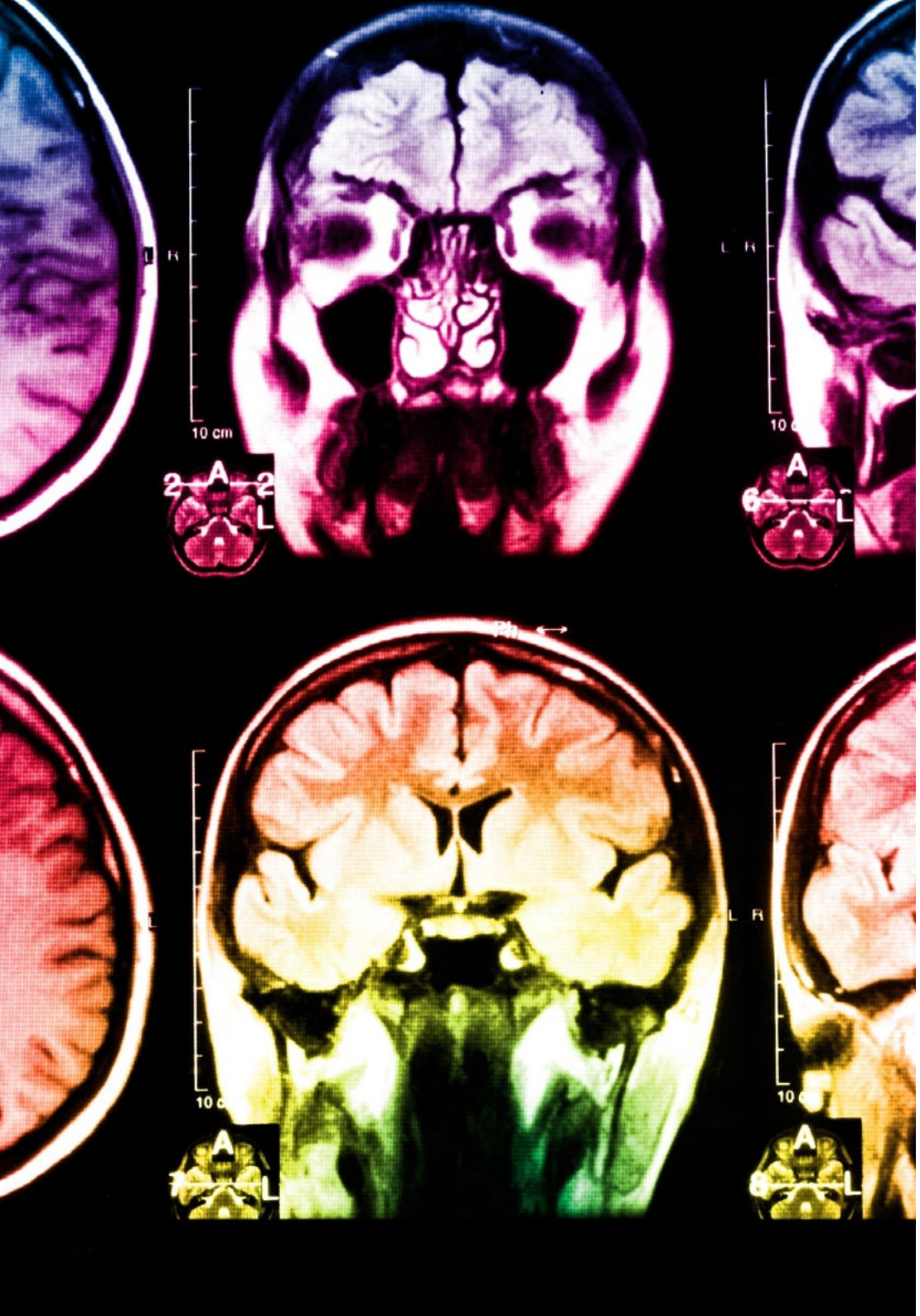
再学习方法

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。

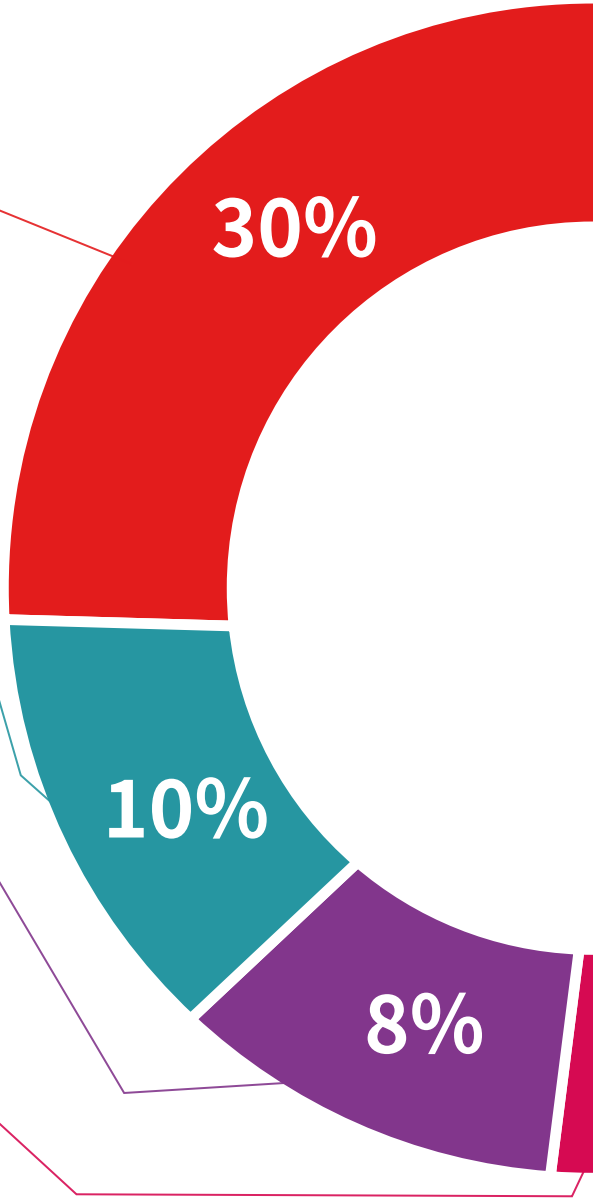
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

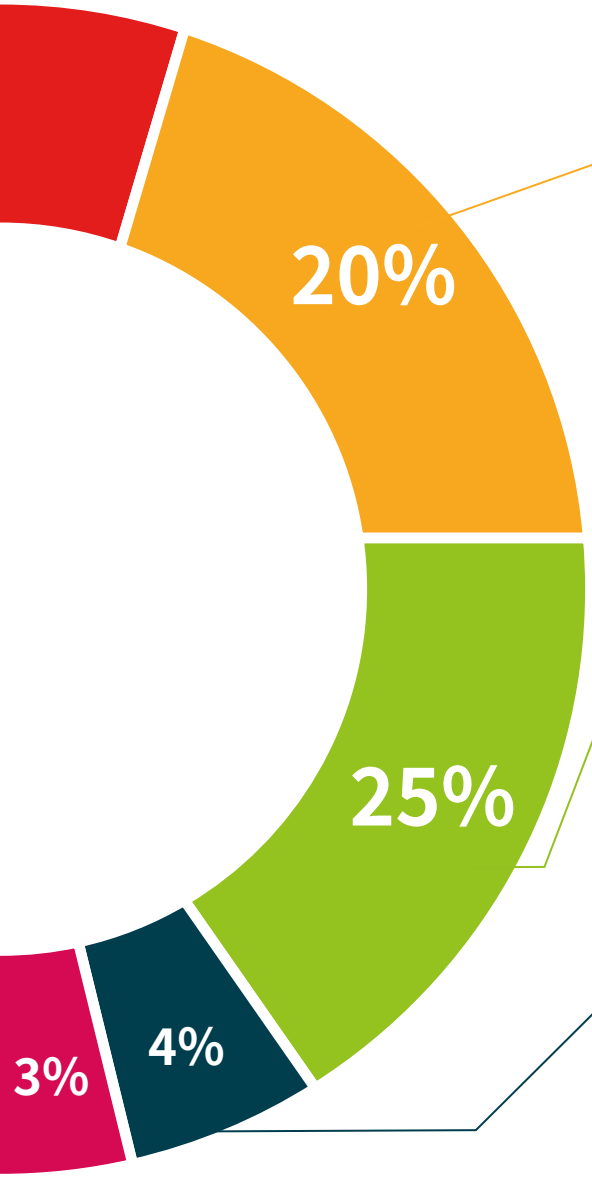
技能和能力的实践

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。

07

学位

在企业中网络安全政策管理校级硕士课程除了保证最严格和最新的培训外，还可以获得由TECH科技大学颁发的校级硕士学位证书。

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**在企业中网络安全政策管理校级硕士**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**校级硕士**学位。

学位由**TECH科技大学**颁发，证明在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：**在企业中网络安全政策管理校级硕士**

官方学时：**1,500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

校级硕士

在企业中网络安全政策管理

这是一个由本大学授予的学位，相当于1,500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


在企业中网络安全政策管理校级硕士

科目类型	小时
必修(OB)	1,500
选修 (OP)	0
外部实习 (PR)	0
硕士论文 (TFM)	0
总计	1,500

教学大纲概况

学期	学科	小时	性质
1°	信息安全管理制度	150	必修
1°	信息安全政策的组织方面	150	必修
1°	信息系统的安全政策 威胁分析	150	必修
1°	实际执行软件和硬件安全政策	150	必修
1°	安全事件管理政策	150	必修
1°	在企业中实施安全和环境安全政策	150	必修
1°	企业中的安全通信政策	150	必修
1°	面对攻击时安全政策的实际执行情况	150	必修
1°	信息系统安全政策中的监测工具	150	必修
1°	实用的安全灾难恢复政	150	必修

Tere Guevara Navarro女士
校长

tech 科学技术大学

*海牙认证。如果学生要求他或她的纸质学位进行海牙认证，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

校级硕士
在企业中网络安全政策管理

- 模式:在线
- 时间:12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

校级硕士
在企业中网络安全政策管理

tech 科学技术大学