

专科文凭 安全与密码学



专科文凭 安全与密码学

- » 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.techitute.com/cn/information-technology/postgraduate-diploma/postgraduate-diploma-security-cryptography

目录

01

介绍

4

02

目标

8

03

课程管理

12

04

结构和内容

16

05

方法

22

06

学历

30

01 介绍

密码学是当今网络安全领域最重要的领域之一。在这一领域,可以利用算法等工具,通过加密过程保护各类信息。各种类型的公司都需要确保其数据的安全,因此他们会寻找这一领域的专业人员,由他们来提供所需的安全标准。该课程是对称密码学、区块密码、量子算法或区块链技术方面最前沿的课程。所有这些都建立在 100% 在线教学系统的基础上,专业人员可以根据个人情况,将学习与工作相结合。





通过本计划, 你将学习到保护客户和雇主数据的最佳加密方法"

密码学是一门不断发展的学科,对专业人才的需求与日俱增。这一领域可以保护各种数字数据,应用于银行、网上商店、各种数据库等领域,对区块链至关重要。因此,专门从事这一领域的工作是当今 IT 专业人员的必修课。

许多公司,不仅仅是技术公司,都需要密码学专家来提高信息的安全性,而本计划正是为了满足这一需求。通过 3 个模块 450 个小时的学习,计算机科学家将能够深入研究密码学的数学基础、信息系统的分析和风险管理方法或针对量子计算的算法保护等问题。

专业人员将能够通过 100% 的在线方法深入学习这个学科,这种方法是专门为学生能够将工作与学习相结合而设计的。此外,该课程将由在密码学领域享有盛誉的教师团队授课,他们将利用各种多媒体资源讲授该课程。

这个**安全与密码学专科文凭**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

“

密码学是 Facebook、Paypal 或亚马逊等公司的支柱产业,区块链技术为其带来了巨大的推动力,因此,专门从事这一领域的工作会带来大量的职业机会”

“

通过使用最好的多媒体材料和由活跃的专业人员组成的教学团队,你将能够学习到应用于计算机安全的密码学的所有关键”

该方案在其教学人员中包括该部门的专业人员,他们将自己的工作经验注入这一培训中,此外还有来自参考协会和著名大学的知名专家。

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。

密码学是当今最重要的IT领域:本课程将通过市场上最好的在线教学,让你专攻密码学。

通过本专科文凭,你将深入了解密码学的方方面面,例如针对量子计算的算法保护。



02 目标

本安全与密码学专科文凭的主要目的是为专业人员提供网络安全领域的最新发展,使他们在完成学业后能够在任何需要该领域专家的公司工作。TECH 为你提供最完整和最新的内容、最灵活的教学系统以及在密码学领域享有盛誉的教师。



“

本课程将帮助你实现所有专业目标，
使你成为一名出色的密码学专家”



总体目标

- ◆ 分析和发展风险的概念
- ◆ 审查基于ISO 31.000的风险管理模式
- ◆ 应用MAGERIT方法来发展模型,并使其更进一步
- ◆ 根据设计新的风险管理方法 敏捷风险管理
- ◆ 基础,从新的业务视角来识别、分析、评估和应对所面临的 风险驱动从而不仅能够在我们的环境中生存,还能推动价值贡献
- ◆ 最大限度地利用设计带来的机遇,消除设计本身可能存在的所有风险
- ◆ 检视密码科学以及与分支的关系:密码学、密码分析、隐写术和隐写分析
- ◆ 根据算法的类型和用途,分析密码学的类型
- ◆ 汇编钥匙管理系统
- ◆ 评估不同的实际应用
- ◆ 检查数字证书
- ◆ 检查公钥基础设施 (PKI)
- ◆ 分析最新趋势和挑战
- ◆ 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.风险分析和 IT 安全环境

- ◆ 以全面的眼光来审视我们所处的环境
- ◆ 确定可能影响我们实现目标的主要风险和机会
- ◆ 根据我们现有的最佳做法来分析风险
- ◆ 评估这些风险和机遇的潜在影响
- ◆ 开发技术,使我们能够以最大限度地贡献价值的方式应对风险和机遇
- ◆ 深入研究不同的风险和价值转移技术
- ◆ 从设计自己的模型中产生价值,用于敏捷的风险管理
- ◆ 检查结果,提出项目和流程管理的持续改进建议 风险驱动管理模式
- ◆ 创新并将一般数据转化为基于风险的决策的相关信息

模块2.信息技术的密码学

- ◆ 汇编基本操作 (XOR、大数、替换和换位) 和各种组件 (单向函数、哈希、随机数生成器)
- ◆ 分析加密技术
- ◆ 开发不同的加密算法
- ◆ 展示数字签名的使用及在数字证书中的应用
- ◆ 评估密钥管理系统和加密密钥长度的重要性
- ◆ 检验密钥推导算法
- ◆ 分析关键的生命周期
- ◆ 评估区块密码和流密码模式
- ◆ 确定伪随机数生成器
- ◆ 开发真实世界的密码学应用案例,如Kerberos、PGP或智能卡
- ◆ 检视相关的协会和机构,如ISO、NIST或NCSC
- ◆ 了解量子计算密码学的挑战

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



不要再等待了:在这个专科文凭中,你可以找到你一直在寻找的专业进步"

03 课程管理

该课程由活跃在密码学领域的顶级专家讲授 3 个模块。因此, 这个专科文凭的师资队伍是其最大的优势之一, 因为其中包括该领域享有盛誉的专家, 他们将向学生传授能够使用最佳加密技术和工具工作的所有秘诀。





由活跃在密码学领域的专业人士组成的
教学团队将指导你完成整个学习过程"

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
- ◆ 教学人员公司业务区块链培训

教师

Gonzalo Alonso, Félix 先生

- ◆ Smart REM Solutions 首席执行官兼创始人
- ◆ 创始合伙人兼风险工程与创新负责人。Dynargy
- ◆ 经理和创始合伙人Risknova (技术专业专家办公室)
- ◆ 科米利亚斯宗座大学 ICAI 工业组织工程学士
- ◆ 毕业于 Universidad Pontificia de Comillas ICAI 工业技术工程专业, 专攻工业电子
- ◆ ICEA保险管理硕士(保险实体合作研究所)



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

Ortega Esteban, Octavio 先生

- ◆ 计算机应用程序程序员和 Web 开发
- ◆ 为客户设计网站和应用程序、卡洛斯三世健康研究所进行的研究用 CRDS、在线商店、Android 应用程序等。
- ◆ 计算机安全教师
- ◆ 加泰罗尼亚开放大学心理学学士
- ◆ 分析、设计和软件解决方案高级大学技术员
- ◆ 高级编程高级大学技术员

04 结构和内容

本安全和密码学专科文凭的学习时间为 6 个月，共 450 个学时。此外，该课程还分为三个模块，计算机科学家将通过这三个模块深入研究信息系统的分析和风险管理方法、基于敏捷方法的信息技术风险地图开发、应用于风险管理的人工智能或应用于区块链的密码学等问题。





通过该课程,你将了解到隐写术的最新内容"

模块1. 风险分析和IT安全环境

- 1.1. 周边分析
 - 1.1.1. 现状分析
 - 1.1.1.1. VUCA 环境
 - 1.1.1.1.1. 变化大
 - 1.1.1.1.2. 不确定
 - 1.1.1.1.3. 复杂
 - 1.1.1.1.4. 模糊
 - 1.1.1.2. BANI 环境
 - 1.1.1.2.1. 易碎
 - 1.1.1.2.2. 焦虑
 - 1.1.1.2.3. 非线性
 - 1.1.1.2.4. 无法理解
 - 1.1.2. 大环境分析PESTEL
 - 1.1.2.1. 政治
 - 1.1.2.2. 经济
 - 1.1.2.3. 社会
 - 1.1.2.4. 技术
 - 1.1.2.5. 生态/环境
 - 1.1.2.6. 法律
 - 1.1.3. 内部情况分析DAFO
 - 1.1.3.1. 目标
 - 1.1.3.2. 威胁
 - 1.1.3.3. 机会
 - 1.1.3.4. 优势
- 1.2. 风险与不确定性
 - 1.2.1. 风险
 - 1.2.2. 风险管理
 - 1.2.3. 风险管理标准
- 1.3. ISO 31,000:2018 风险管理指南
 - 1.3.1. 目标
 - 1.3.2. 原则
 - 1.3.3. 框架
 - 1.3.4. 过程
- 1.4. 信息系统风险分析和管理方法 (MAGERIT)
 - 1.4.1. MAGERIT 方
 - 1.4.1.1. 目标
 - 1.4.1.2. 方法
 - 1.4.1.3. 要素
 - 1.4.1.4. 技术
 - 1.4.1.5. 可用工具 (PILAR)
- 1.5. 网络风险转移
 - 1.5.1. 风险转移
 - 1.5.2. 网络风险类型
 - 1.5.3. 网络风险保险
- 1.6. 风险管理的敏捷方法
 - 1.6.1. 敏捷方法
 - 1.6.2. Scrum 风险管理
 - 1.6.3. 敏捷风险管理
- 1.7. 风险管理技术
 - 1.7.1. 人工智能应用于风险管理
 - 1.7.2. 区块链和密码学保值方法
 - 1.7.3. 量子计算机会或威胁
- 1.8. 基于敏捷方法的 IT 风险图的准备
 - 1.8.1. 敏捷环境中概率和影响的表示
 - 1.8.2. 作为价值威胁的风险
 - 1.8.3. 基于 KRI 的项目管理和敏捷流程的再进化
- 1.9. 风险管理中的风险驱动
 - 1.9.1. 风险驱动
 - 1.9.2. 风险管理中的风险驱动
 - 1.9.3. 开发风险驱动的业务管理模式

- 1:10. IT风险管理的创新与数字化转型
 - 1.10.1. 敏捷风险管理是业务创新的源泉
 - 1.10.2. 将数据转化为对决策有用的信息
 - 1.10.3. 通过风险的公司整体愿景

模块2. 信息技术的密码学

- 2.1. 密码学
 - 2.1.1. 密码学
 - 2.1.2. 数学基础
- 2.2. 密码学
 - 2.2.1. 密码学
 - 2.2.2. 密码分析
 - 2.2.3. 隐写术和隐写分析
- 2.3. 密码协议
 - 2.3.1. 基本块
 - 2.3.2. 基本协议
 - 2.3.3. 中间协议
 - 2.3.4. 高级协议
 - 2.3.5. 公开协议
- 2.4. 密码技术
 - 2.4.1. 密钥长度
 - 2.4.2. 密钥处理
 - 2.4.3. 算法类型
 - 2.4.4. 汇总函数哈希
 - 2.4.5. 伪随机数发生器
 - 2.4.6. 算法的使用
- 2.5. 对称密码学
 - 2.5.1. 分组密码
 - 2.5.2. DES (数据加密标准)
 - 2.5.3. RC4算法
 - 2.5.4. AES (高级加密标准)
 - 2.5.5. 分组密码的组合
 - 2.5.6. 密钥派生
- 2.6. 非对称密码学
 - 2.6.1. Diffie-Hellman
 - 2.6.2. DSA (数字签名算法)
 - 2.6.3. RSA (Rivest, Shamir 和 Adleman)
 - 2.6.4. 椭圆曲线
 - 2.6.5. 非对称密码学类型
- 2.7. 数字证书
 - 2.7.1. 电子签名
 - 2.7.2. X509 证书
 - 2.7.3. 公钥基础设施 (PKI)
- 2.8. 执行
 - 2.8.1. Kerberos
 - 2.8.2. IBM CCA
 - 2.8.3. 相当好的隐私 (PGP)
 - 2.8.4. ISO 认证框架
 - 2.8.5. SSL 和 TLS
 - 2.8.6. 支付方式中的智能卡 (EMV)
 - 2.8.7. 手机协议
 - 2.8.8. 区块链
- 2.9. 隐写术
 - 2.9.1. 隐写术
 - 2.9.2. 隐写分析
 - 2.9.3. 应用和用途
- 2:10. 量子密码学
 - 2.10.1. 量子算法
 - 2.10.2. 保护算法免受量子计算
 - 2.10.3. 量子密钥分发

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. 第 1 阶段: 组织的分析
 - 3.5.2. 第 2 阶段: 确定连续性策略
 - 3.5.3. 第 3 阶段: 应急响应
 - 3.5.4. 第 4 阶段: 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



“各行各业的公司都希望依靠你们来保护其最宝贵的数据”

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,图像记忆,而且知道我们学到东西的地方和背景,这是我们记住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。



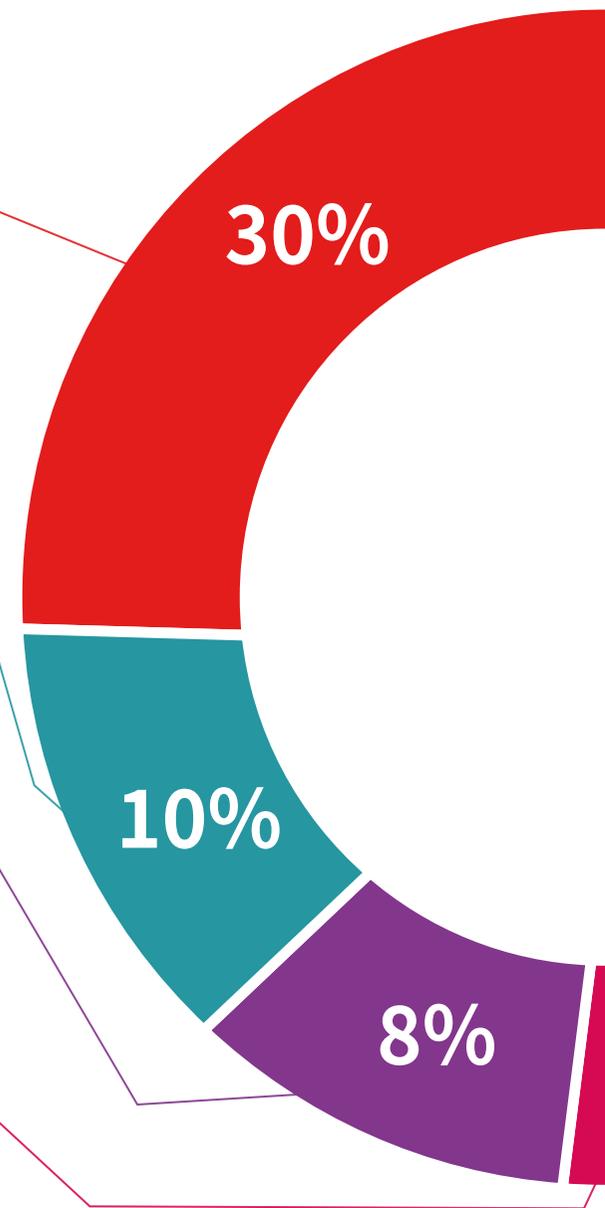
技能和能力的实践

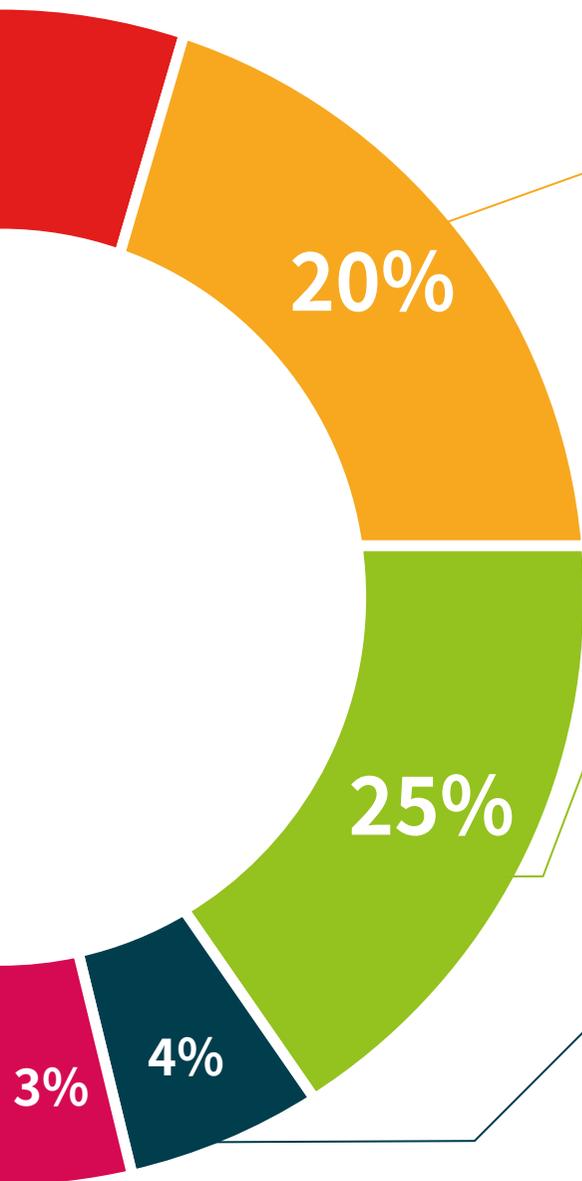
你将开展活动以发展每个学科领域的具体能力和技能。在我们所处的全球化框架内,我们提供实践和氛围帮你取得成为专家所需的技能和能力。



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

安全与密码学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**安全与密码学专科文凭**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:**安全与密码学专科文凭**

官方学时:**450小时**



健康 信心 未来 人 导师
教育 信息 教学
保证 资格认证 学习
机构 社区 科技 承诺
个性化的关注 现在 创新
知识 网页 培 质量
网上教室 发展 语言

tech 科学技术大学

专科文凭
安全与密码学

- » 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 安全与密码学