

专科文凭

新兴科技的网络安全



专科文凭 新兴科技的网络安全

- » 模式:在线
- » 时长:6个月
- » 学位:TECH Global University
- » 认证:ECTS 18
- » 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-diploma/postgraduate-diploma-cybersecurity-emerging-technologies

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

最近出现了许多科技,并迅速普及。这不仅为企业,用户和客户提供了新的服务,也带来了安全问题。科技新兴的性质决定了它们处于不断发展之中,尚未达到最佳保护状态,因此容易受到攻击。为了应对这一挑战,我们制定了这一计划,使计算机科学家能够学习应用于物联网最佳网络安全方法:云计算和区块链。通过这种方式,你将提升自己的专业形象,为应对当前和未来的数字安全挑战做好准备。



通过本专科文凭的学习, 您将掌握应用于云计算、区块链或物联网的网络安全专业技能 成为最优秀的科技公司争相聘用的专业人才”

新兴科技将继续存在。它们出现在需要解决各种问题的时候。例如，物联网正在发展成为许多人生活中不可或缺的元素。区块链 还有助于分散许多流程，而 云计算 则可确保在任何地方，通过简单的网络连接即可获得各种资源，特别是数据或应用程序。

由于这些都是非常有用的元素和服务，其受欢迎程度正在迅速增长，这就造成了平衡的缺失，因为它们往往没有足够的安全性，因为它们是尚未得到 100%开发的技术。因此，越来越多的公司，无论是在电子领域还是其他领域，都在寻找专门从事这些工具网络安全的专业人员。

因此，本专科文凭探讨了网络安全技术的所有可能性，确保计算机科学家能够在这一领域进行全面深入的学习，为其职业生涯带来决定性的专业提升。

所有这一切，都是通过专门为在职专业人员设计的在线教学系统实现的，他们将能够以一种舒适简单的方式将工作与学习结合起来。此外，你还将拥有由网络安全这一重要领域的真正专家组成的最佳教学团队。

这个**新兴科技的网络安全专科文凭**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



各类公司都需要专家为其区块链或物联网项目提供最佳安全性"

“

最好的在线教学系统供你使用, 这样你就可以按照自己的节奏学习, 没有死板的时间表, 也不会影响你的工作”

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融入到培训中, 还有来自知名企业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。

通过本计划, 你将能够了解更多有关最佳加密方法或现有云基础设施类型的信息。

新兴科技是现在也是未来: 学好专业课程, 立即改善你的职业前景。



02 目标

本新兴科技的网络安全专科文凭的主要目标是将计算机科学家培养成该领域的参考专家,为任何希望以全面安全的方式处理区块链或云计算项目的公司提供完美的解决方案。完成本课程后,你将具备完美的专业素质,以适应新的技术和数字环境。





“

完成本专科文凭后, 你将成为所在环境中最受欢迎的专业人士”



总体

- ◆ 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
- ◆ 考察公钥基础设施 (PKI)
- ◆ 分析最新趋势和挑战
- ◆ 检视在云中部署企业服务时设计安全策略的过程
- ◆ 识别云安全的领域
- ◆ 分析每个安全领域的服务和工具
- ◆ 评估不同公共云供应商在具体实施上的差异
- ◆ 评估物联网连接选项,以解决一个项目,重点是LPWAN技术
- ◆ 介绍用于物联网的主要LPWAN技术的基本规格
- ◆ 制定每种LPWAN技术的安全规范
- ◆ LPWAN技术的安全性比较分析





具体目标

模块 1. 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 2. 云环境的安全问题

- ◆ 识别公共云基础设施部署的风险
- ◆ 界定安全要求
- ◆ 为云计算部署制定一个安全计划
- ◆ 确定为实施安全计划所要部署的云服务
- ◆ 确定预防机制所需的操作
- ◆ 建立记录和监测系统的准则
- ◆ 提出事件应对行动的建议

模块3. 物联网设备通信的安全性

- ◆ 介绍简化的物联网架构
- ◆ 解释通用连接技术和物联网连接技术之间的区别
- ◆ 建立物联网连接的铁三角概念
- ◆ 分析LoRaWAN技术、NB-IoT技术和WiSUN技术的安全规范
- ◆ 为每个项目选择合适的物联网技术提供依据



你的所有职业目标都将指日可待: 入学并成为新兴科技网络安全专家"

03 课程管理

当前的复杂形势要求专业人员不断更新和深化自己的知识。专业人员必须不断更新和深化自己的知识。新兴科技不仅开辟了新天地,而且随着新技术的发展而不断变革。因此,必须拥有该领域最优秀的专家,而这个专科文凭就拥有这些专家,这样计算机科学家就能从活跃的专业人士的教学中了解到所有最新发展。



“

在网络安全领域工作的最有经验的教师将为你提供最先进的知识和技术”

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

Gómez Rodríguez, Antonio 先生

- ◆ Oracle 云端解决方案工程师
- ◆ Sopra 集团项目总监
- ◆ Everis 项目总监
- ◆ 公司的文化项目管理负责人安达卢西亚文化部
- ◆ 信息系统分析师Sopra Group
- ◆ 加泰罗尼亚理工大学电信工程学士学位
- ◆ 加泰罗尼亚理工学院信息技术和系统专业的研究生学位
- ◆ 拉萨尔商学院电子商务硕士

del Valle Arias, Jorge 先生

- ◆ Itron Inc 西班牙智慧城市业务增长经理
- ◆ 物联网顾问
- ◆ Diode Spain 物联网部门总监
- ◆ Aicox Solutions 物联网和蜂窝销售经理
- ◆ 传感器智能创始人兼CEO
- ◆ Codium Networks 运营总监
- ◆ Aitemin 电子领域负责人
- ◆ 马德里理工大学电信工程师
- ◆ 马德里拉萨尔国际研究生院行政工商管理硕士

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



你将能够适当地应对所有类型的网络安全威胁。报名参加,成为优秀专家"

04

结构和内容

本新兴科技的网络安全专科文凭由 3 个专业模块组成, 将通过 540 个小时的强化学习来完成。从这一结构出发, 计算机科学家将能够深入研究网络安全的相关方面, 如密码学的数学基础、算法在安全中的应用、公共云的安全以及物联网的主要安全漏洞。





“

在本计划中,有关应用于新兴科技的网络安全的内容最为完整。不要再等了,赶紧报名吧”

模块 1. 信息技术的密码学

- 1.1. 密码学
 - 1.1.1. 密码学
 - 1.1.2. 数学基础
- 1.2. 密码学
 - 1.2.1. 密码学
 - 1.2.2. 密码分析
 - 1.2.3. 隐写术和隐写分析
- 1.3. 密码协议
 - 1.3.1. 基本块
 - 1.3.2. 基本协议
 - 1.3.3. 中间协议
 - 1.3.4. 高级协议
 - 1.3.5. 公开协议
- 1.4. 密码技术
 - 1.4.1. 密钥长度
 - 1.4.2. 密钥处理
 - 1.4.3. 算法类型
 - 1.4.4. 汇总函数哈希
 - 1.4.5. 伪随机数发生器
 - 1.4.6. 算法的使用
- 1.5. 对称密码学
 - 1.5.1. 分组密码
 - 1.5.2. DES (数据加密标准)
 - 1.5.3. RC4算法
 - 1.5.4. AES (高级加密标准)
 - 1.5.5. 分组密码的组合
 - 1.5.6. 密钥派生



- 1.6. 非对称密码学
 - 1.6.1. Diffie-Hellman
 - 1.6.2. DSA (数字签名算法)
 - 1.6.3. RSA (Rivest, Shamir y Adleman)
 - 1.6.4.. 椭圆曲线
 - 1.6.5. 非对称密码学类型
- 1.7. 数字证书
 - 1.7.1. 电子签名
 - 1.7.2. X509 证书
 - 1.7.3. 公钥基础设施 (PKI)
- 1.8. 执行
 - 1.8.1. Kerberos
 - 1.8.2. IBM CCA
 - 1.8.3. 相当好的隐私 (PGP)
 - 1.8.4. ISO 认证框架
 - 1.8.5. SSL 和 TLS
 - 1.8.6. 支付方式中的智能卡 (EMV)
 - 1.8.7. 手机协议
 - 1.8.8. 区块链
- 1.9. 隐写术
 - 1.9.1. 隐写术
 - 1.9.2. 隐写分析
 - 1.9.3. 应用和用途
- 1.10. 量子密码学
 - 1.10.1. 量子算法
 - 1.10.2. 保护算法免受量子计算
 - 1.10.3. 量子密钥分发

模块 2.云环境的安全问题

- 2.1. 云计算环境中的安全性
 - 2.1.1. 云计算环境中的安全性
 - 2.1.2. 云计算环境中的安全性安全威胁和风险
 - 2.1.3. 云计算环境中的安全性关键安全方面
- 2.2. 云基础设施类型
 - 2.2.1. 公众
 - 2.2.2. 私人
 - 2.2.3. 混合
- 2.3. 共享管理模式
 - 2.3.1. 供应商管理的安全元素
 - 2.3.2. 客户管理的项目
 - 2.3.3. 安全策略的定义
- 2.4. 预防机制
 - 2.4.1. 认证管理系统
 - 2.4.2. 授权管理系统:访问策略
 - 2.4.3. 密钥管理系统
- 2.5. 系统安全
 - 2.5.1. 存储系统的安全
 - 2.5.2. 保护数据库系统
 - 2.5.3. 传输中数据的安全性
- 2.6. 基础设施保护
 - 2.6.1. 安全网络设计和实施
 - 2.6.2. 计算资源安全
 - 2.6.3. 基础设施保护的资源和工具
- 2.7. 检测威胁和攻击
 - 2.7.1. 审计、日志和监控系统
 - 2.7.2. 事件和警报系统
 - 2.7.3. SIEM系统
- 2.8. 事件响应
 - 2.8.1. 事件响应计划
 - 2.8.2. 业务连续性
 - 2.8.3. 同性质事件的取证分析和补救

- 2.9. 公共云的安全性
 - 2.9.1. AWS(亚马逊网络服务)
 - 2.9.2. Microsoft Azure
 - 2.9.3. 谷歌GCP
 - 2.9.4. Oracle 云
- 2.10. 法规和合规性
 - 2.10.1. 遵守安全法规
 - 2.10.2. 风险管理
 - 2.10.3. 组织的人员和流程

模块3.物联网设备通信安全

- 3.1. 从遥测到物联网
 - 3.1.1. 遥测
 - 3.1.2. M2M 连接
 - 3.1.3. 遥测民主化
- 3.2. 物联网参考模型
 - 3.2.1. 物联网参考模型
 - 3.2.2. 简化的物联网架构
- 3.3. 物联网安全漏洞
 - 3.3.1. 物联网设备
 - 3.3.2. 物联网设备使用案例
 - 3.3.3. 物联网设备漏洞
- 3.4. 物联网连接
 - 3.4.1. PAN、LAN、WAN 网络
 - 3.4.2. 非物联网无线技术
 - 3.4.3. LPWAN 无线技术
- 3.5. LPWAN 技术
 - 3.5.1. LPWAN 网络的铁三角
 - 3.5.2. 免费频段对比授权频段
 - 3.5.3. LPWAN 技术选项



- 3.6. LoRaWAN 技术
 - 3.6.1. LoRaWAN 技术
 - 3.6.2. LoRaWAN 用例生态系统
 - 3.6.3. LoRaWAN 中的安全性
- 3.7. 西格福克斯技术
 - 3.7.1. 西格福克斯技术
 - 3.7.2. 西格福克斯用例生态系统
 - 3.7.3. 西格福克斯的安全性
- 3.8. 蜂窝物联网技术
 - 3.8.1. 蜂窝物联网技术 (NB-IoT 和 LTE-M)
 - 3.8.2. 蜂窝物联网用例生态系统
 - 3.8.3. 蜂窝物联网安全
- 3.9. WiSUN技术
 - 3.9.1. WiSUN技术
 - 3.9.2. WiSUN 用例生态系统
 - 3.9.3. WiSUN的安全
- 3.10. 其他物联网技术
 - 3.10.1. 其他物联网技术
 - 3.10.2. 其他物联网技术的用例和生态系统
 - 3.10.3. 其他物联网技术的安全性



最优秀的教师将以最新的内容为你介绍新兴科技中的安全问题"

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。



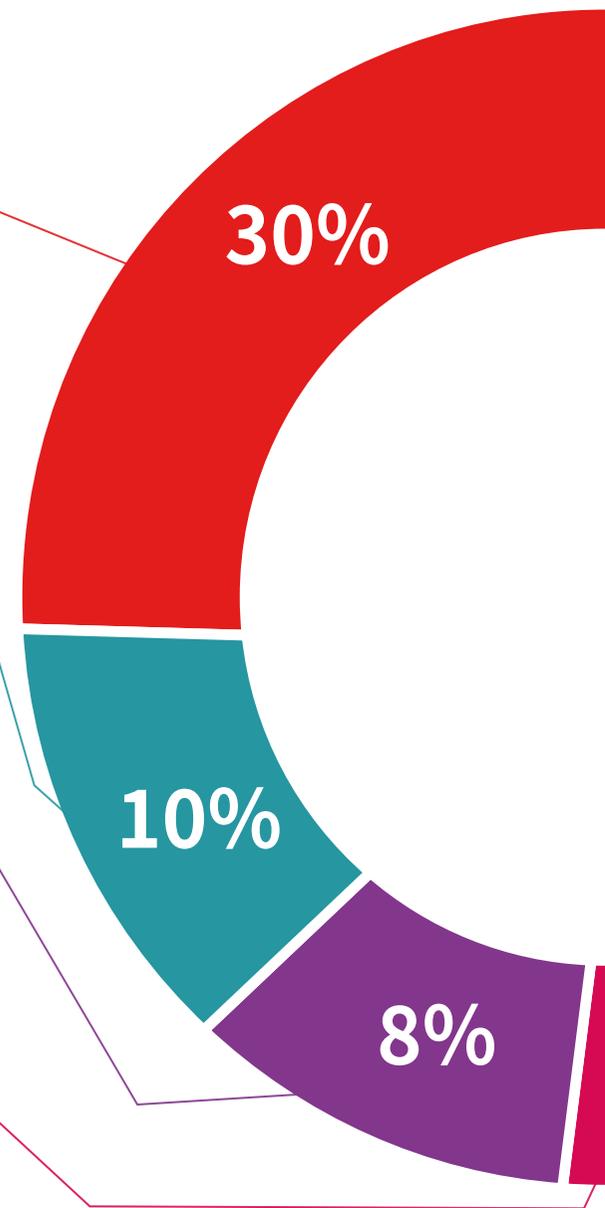
技能和能力的实践

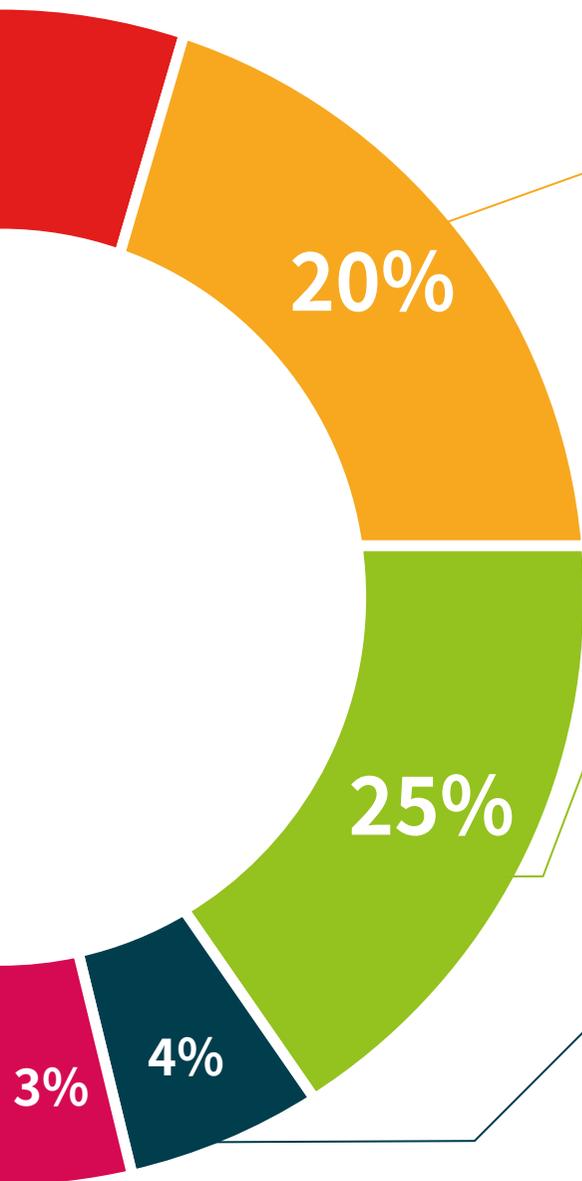
你将开展活动以发展每个学科领域的具体能力和技能。在我们所处的全球化框架内,我们提供实践和氛围帮你取得成为专家所需的技能和能力。



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

新兴科技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 Global University颁发的大学课程学位证书。



“

成功完成该课程并获得无需舟车劳顿或办理手续 即可获得大学学位”

这个课程将使您有机会获得 **TECH Global University** 认可的**新兴科技的网络安全专科文凭**学位。TECH Global University 是全球最大的数字大学。

TECH Global University 是一所经安道尔政府 ([官方公报](#)) 公开认可的欧洲官方大学。自2003年以来,安道尔已成为欧洲高等教育区 (EEES) 的一部分。该高等教育区是欧盟推动的一个倡议,旨在组织国际教育框架,并协调成员国的高等教育系统。该项目促进了共同价值观的推广,实施了共同工具,并加强了质量保证机制,以促进学生、研究人员和学者之间的合作和流动。

TECH Global University 的专业学位是一个欧洲的继续教育和职业更新项目,确保学生在其知识领域获得能力,并为完成该项目的学生赋予了高度的学术价值。

学位:新兴科技的网络安全专科文凭

模式:在线

时长: 6 个月

认证: ECTS 18



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
知识 网页 培
网上教室 发展 语言

tech global university

质量
专科文凭
新兴科技的网络安全

- » 模式:在线
- » 时长:6个月
- » 学位:TECH Global University
- » 认证:ECTS 18
- » 课程表:自由安排时间
- » 考试模式:在线

专科文凭

新兴科技的网络安全