商学院校级硕士
企业的网络安|全政策管理

tech 科学技术大学

tech 科学技术大学

商学院校级硕士
企业的网络安全政策管理

- 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**
- 目标群体: **大学毕业生,大学课程和学位持有者，以前在卫生科学,社会和法律科学,行政和商业领域完成过任何。**

网络访问: **www.techtitute.com/cn/school-of-business/master/corporate-cybersecurity-policy-management**

目录

01

欢迎

今天，由于网络攻击造成的损失估计有数百万，甚至远超数百万。网络攻击的风险如此之大，甚至国家也可能成为网络事件的目标。这强调了拥有专门管理网络安全政策的管理人员的重要性，他们在组织,实施和监测工具方面拥有适当的知识，以协调所有网络安全努力。该课程通过提供高质量的信息安全解决课程，使管理人员能够以先进的安全和知识应对不确定的情况。通过基于真实案例研究的详尽理论内容，你将获得一个关于网络安全管理人员必须履行的所有职能的现代和全面的观点。此外，所有这些都是以100%的在线形式进行的，没有面对面的课程和预先设定的时间表，具有完全的灵活性。

企业的网络安全政策管理商学院校级硕士。
TECH科技大学

它为你的网络安全政策带来了不可估量的价值，了解它的所有细微差别，从安全系统本身到威胁分析的做法，这将为你提供在你的组织中占据优势的钥匙”

02

为什么在TECH学习?

TECH是世界上最大的100%在线商业学校。它是一所精英商学院，具有最大的学术需求模式。一个国际高绩效和管理技能强化培训的中心。

TECH是一所站在技术前沿的大学，它将所有资源交给学生支配，以帮助他们取得商业成功"

在TECH科技大学

创新

该大学提供一种在线学习模式，将最新的教育科技与最大的教学严谨性相结合。一种具有最高国际认可度的独特方法，将为学生提供在不断变化的世界中发展的钥匙，在这个世界上，创新必须是所有企业家的基本承诺。

“由于在节目中加入了创新的互动式多视频系统，被评为 "微软欧洲成功案例"。

最高要求

TECH的录取标准不是经济的在这所大学学习没有必要进行大量投资。然而，为了从TECH毕业，学生的智力和能力的极限将受到考验。该机构的学术标准非常高。

95% | **TECH学院的学生成功完成学业**

联网

来自世界各地的专业人员参加TECH，因此，学生将能够建立一个庞大的联系网络，对他们的未来很有帮助。

+100,000
每年培训的管理人员

+200
不同国籍的人

赋权

学生将与最好的公司和具有巨大声望和影响力的专业人士携手成长。TECH已经与7大洲的主要经济参与者建立了战略联盟和宝贵的联系网络。

+500 | **与最佳公司的合作协议**

人才

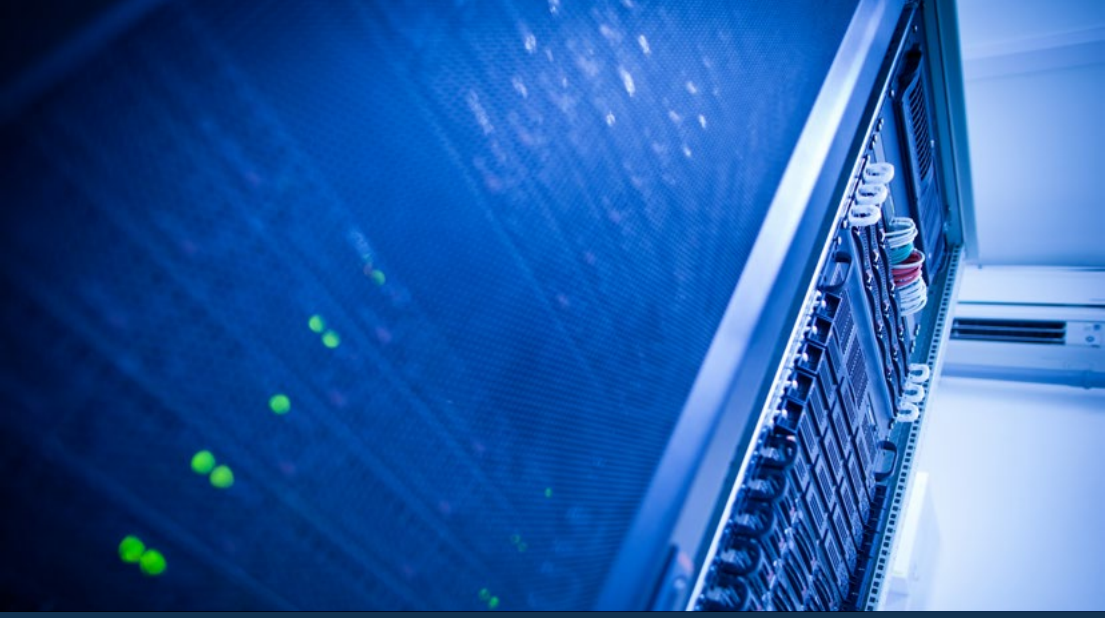
该计划是一个独特的建议，旨在发挥学生在商业领域的才能。这是一个机会，你可以利用它来表达你的关切和商业愿景。

TECH帮助学生在这个课程结束后向世界展示他们的才华。

多文化背景

通过在TECH学习，学生将享受到独特的体验。你将在一个多文化背景下学习。在一个具有全球视野的项目中，由于该项目，你将能够了解世界不同地区的工作方式，收集最适合你的商业理念的创新信息。

TECH的学生来自200多个国家。



向最好的人学习

TECH教学团队在课堂上解释了导致他们在其公司取得成功的原因，在一个真实，活泼和动态的环境中工作。全力以赴提供优质专业的教师，使学生在事业上有所发展，在商业世界中脱颖而出。

来自20个不同国籍的教师。

> 在TECH，你将有机会接触到学术界最严格和最新的案例研究"

TECH追求卓越，为此，有一系列的特点，使其成为一所独特的大学:

分析报告

TECH探索学生批判性的一面，他们质疑事物的能力，他们解决问题的能力和他们的人际交往能力。

优秀的学术成果

TECH为学生提供最好的在线学习方法。大学将再学习方法（国际公认的研究生学习方法）与哈佛大学商学院的案例研究相结合。传统和前卫在一个艰难的平衡中，在最苛刻的学术行程中。

规模经济

TECH是世界上最大的网上大学。它拥有超过10,000个大学研究生课程的组合。而在新经济中，**数量+技术=颠覆性价格**。这确保了学习费用不像在其他大学那样昂贵。

03

为什么选择我们的课程?

完成科技课程意味着在高级商业管理领域取得职业成功的可能性倍增。

这是一个需要努力和奉献的挑战，但它为我们打开了通往美好未来的大门。学生将从最好的教学团队和最灵活，最创新的教育方法中学习。

我们拥有最著名的教师队伍和市场上最完整的教学大纲，这使我们能够为您提供最高学术水平的培训"

该方案将提供众多的就业和个人利益,包括以下内容。

01

对学生的职业生涯给予明确的推动

通过在TECH学习,学生将能够掌握自己的未来,并充分开发自己的潜力。完成该课程后,你将获得必要的技能,在短期内对你的职业生涯作出积极的改变。

本专业70%的学员在不到2年的时间内实现了职业的积极转变。

02

制定公司的战略和全球愿景

TECH提供了一般管理的深刻视野,以了解每个决定如何影响公司的不同职能领域。

我们对公司的全球视野将提高你的战略眼光。

03

巩固高级商业管理的学生

在TECH学习,为学生打开了一扇通往非常重要的专业全景的大门,使他们能够将自己定位为高级管理人员,对国际环境有一个广阔的视野。

你将在100多个高层管理的真实案例中工作。

04

承担新的责任

在该课程中,将介绍最新的趋势,进展和战略,以便学生能够在不断变化的环境中开展专业工作。

45%的受训人员在内部得到晋升。

05

进入一个强大的联系网络

TECH将其学生联系起来，以最大限度地增加机会。有同样关注和渴望成长的学生。你将能够分享合作伙伴，客户或供应商。

你会发现一个对你的职业发展至关重要的联系网络。

06

以严格的方式开发公司项目

学生将获得深刻的战略眼光，这将有助于他们在考虑到公司不同领域的情况下开发自己的项目。

我们20%的学生发展自己的商业理念。

07

提高软技能和管理技能

TECH帮助学生应用和发展他们所获得的知识，并提高他们的人际交往能力，使他们成为有所作为的领导者。

提高你的沟通和领导能力，为你的职业注入活力。

08

成为一个独特社区的一部分

学生将成为由精英经理人，大公司，著名机构和来自世界上最著名大学的合格教授组成的社区的一部分：TECH科技大学社区。

我们给你机会与国际知名的教授团队一起进行专业学习。

04

目标

网络安全是任何现代公司发展的一个重要方面，该计划的目标是提供尽可能最好的网络安全政策管理培训。为此，信息技术专家小组编制了全面的教学材料，完全集中于提高管理人员的技能,能力和素质。

通过学习最有效的网络安全政策的来龙去脉来领导你的组织的网络安全”

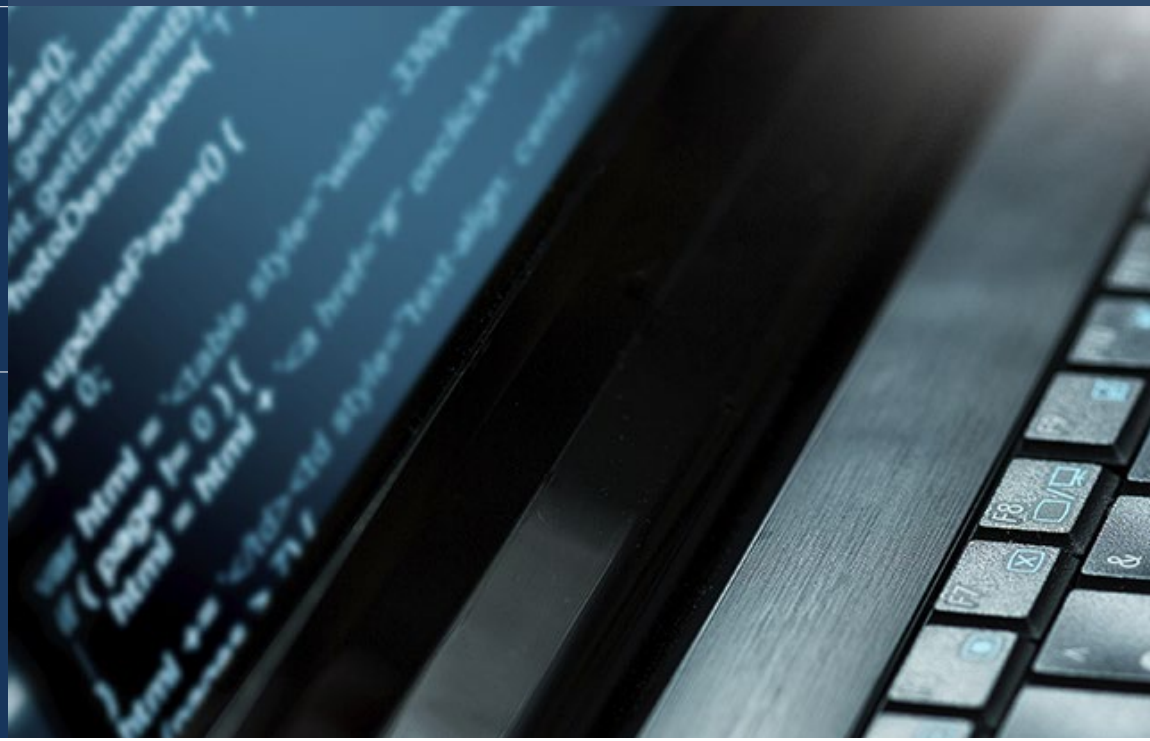
TECH将其学生的目标作为自己的目标。
我们一起工作你实现这些目标。
企业的网络安全政策管理商学院校级硕士将培训学生：

01 加深对关键信息安全概念的理解

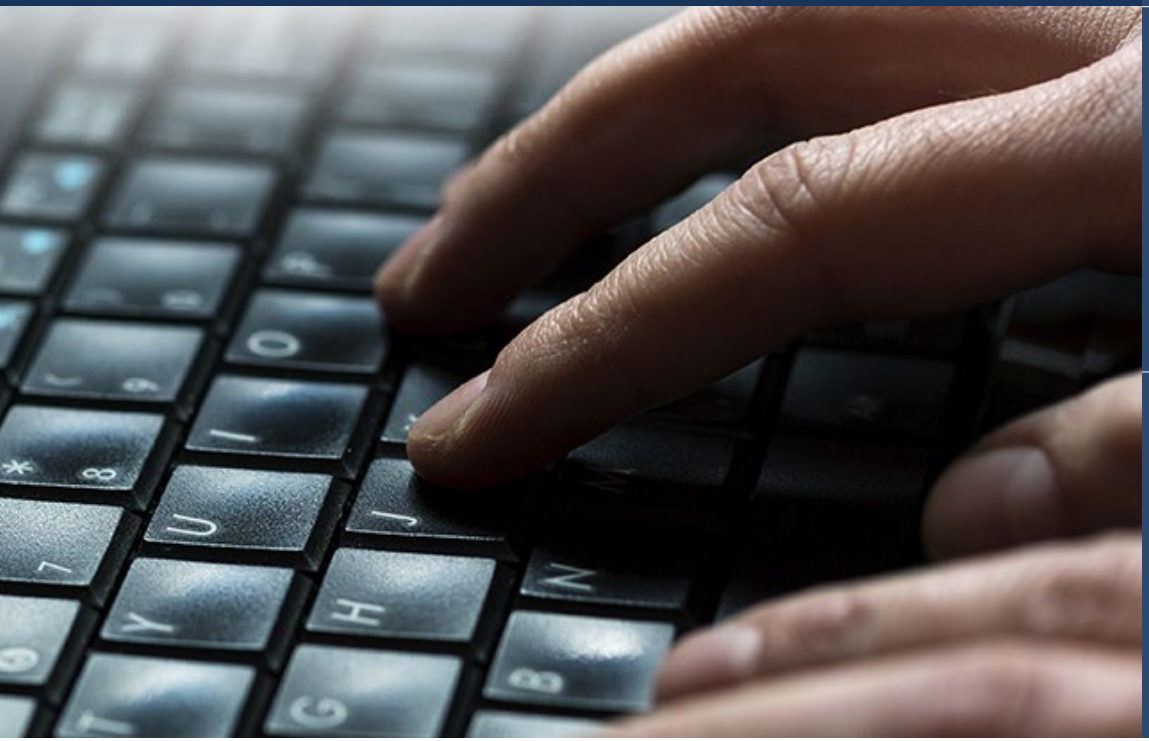
02 分析目前适用于SGSI的法规和标准

03 在公司实施SGSI

04 确定安全管理系统的实施应涵盖哪些部门



05 制定必要的措施以确保良好的信息安全实践



06 确定什么是认证和识别

07 分析现有的不同认证方法和它们的实际实施

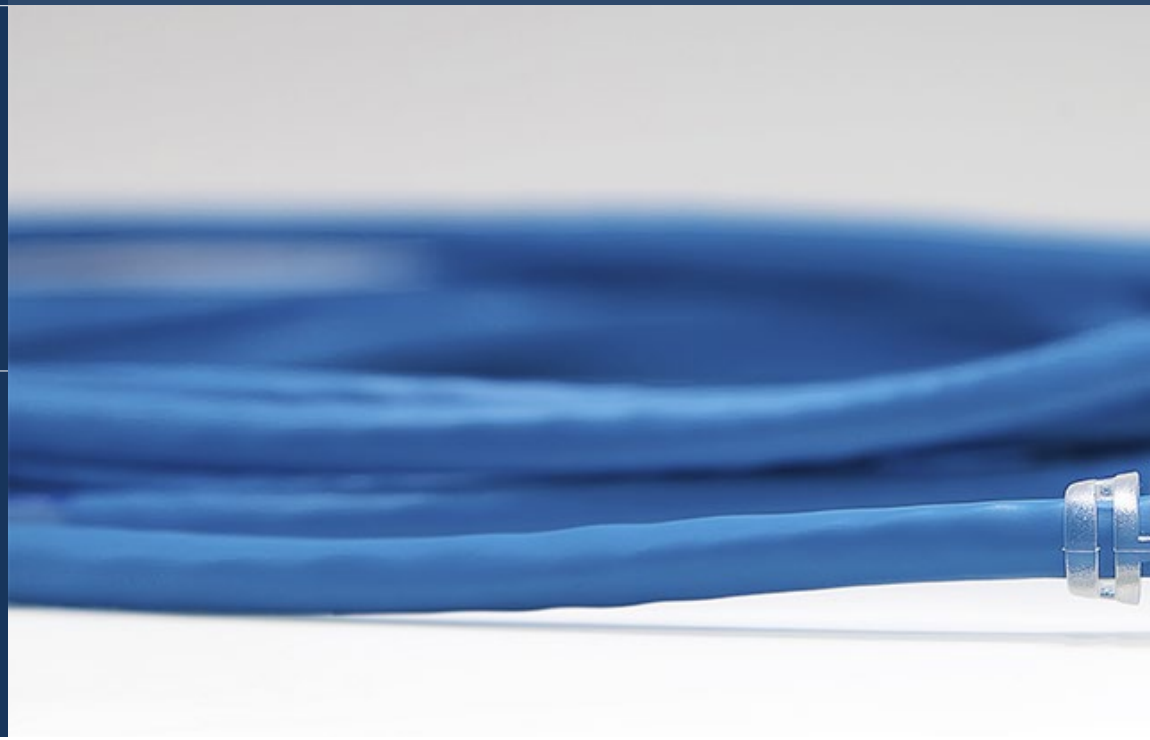
08 对软件和系统实施正确的访问控制政策

09 发展关于如何管理IT安全事件引起的事件的专业知识

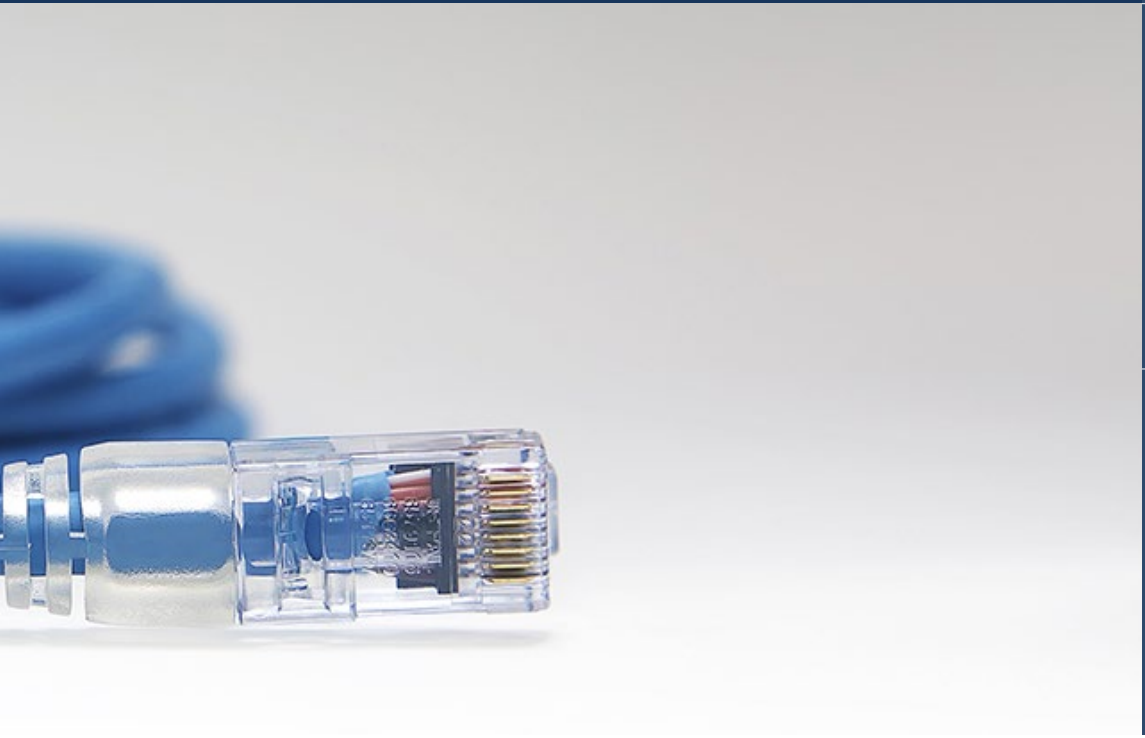
10 分析安全区域和安全周界这一术语

11 分析通信网络中使用的不同加密算法

12 确定对我们信息系统的不同实际攻击



13 评估不同的安全策略以减轻攻击的影响



14 制定监测和实施指标的概念

15 产生关于信息安全连续性概念的专业知识

16 确定什么是密码学和密码学的类型

05

能力

为了进行适当的网络安全政策管理，必须要有很好的组织能力，以及在IT和技术方面的卓越知识和能力。这就是为什么在整个课程中，管理人员不仅可以找到一个有用的IT安全管理参考指南，而且还可以看到他或她的领导和行政管理技能得到加强。

您将完善必要的技能，以突出作为网络安全政策专家的管理人员的地位，为您占据最重要的管理职位提供优势”

01 确定SGSI对实体内部组织的参与及其状态

02 制定公司的安全政策

03 确定我们必须与信息系统供应商和维护部门实施哪些措施

04 生成有关威胁控制的专业知识

05 确定预防性威胁管理的阶段

06 制定网络威胁分析的方法

07 按影响和严重程度对威胁进行分类

08 设计一种分析和预防控制威胁的专有方法

09 对网络和服务实施正确的访问控制政策

10 分析正确处理安全事件的重要性

11 汇编现有的不同生物识别系统

12 检查生物识别和生物识别系统

13 在CPDS中实施各种正确的物理安全策略和物理访问控制系统

14 实施安全网络

15 审查移动平台和物联网的漏洞以及如何避免这些漏洞

16 建立社会工程类型并学会缓解它们

17 分析监测和实施指标的概念

18 确定信息安全连续性的必要性

06

结构和内容

TECH根据 再学习, 方法设计了这一课程, 这意味着经理人不必花很长时间的学习来获得所有建议的知识。网络安全政策中的关键术语和概念在整个学位中以自然和重申的方式给出, 这使得学习过程更有进步性。

你将每天24小时自由进入虚拟教室，能够根据自己的兴趣选择和调整学习进度”

教学大纲

TECH科技大学的企业的网络安全政策管理商学院校级硕士一个强化课程，为学生面对环境管理领域的挑战和商业决策做好准备。

这个公司的企业的网络安全政策管理商学院校级硕士的内容旨在促进技能的发展，以便在不确定的环境中进行更严格的决策。

该商学院校级硕士深入处理数字世界，这一环境中的安全问题以及在公司建立电子商务，旨在培养从战略,国际和创新角度理解公司网络安全政策管理的专业人员。

该商学院校级硕士为期12个月，分为10个内容模块:

模块1. 开发一个信息安全管理系统（SGSI）

模块2. 信息安全政策的组织方面

模块3. 计算机系统威胁分析的安全政策

模块4. 软件和硬件中安全策略的实际实施

模块5. 安全事件管理政策

模块6. 在公司实施实体和环境安全政策

模块7. 企业中的安全通信政策

模块8. 面对攻击时安全策略的实际实施

模块9. 信息系统安全政策中的监测工具

模块10. 实用的安全灾难恢复政策

在哪里,什么时候,如何进行?

TECH 提供了完全在网上发展这个企业的网络安全政策管理商学院校级硕士可能性。在12个月的专业学习期间,学生可以随时访问本课程的所有内容,这将使他们能够自我管理他们的学习时间。

一个独特的,关键的,决定性的教育经历,以促进你的专业发展,实现明确的飞跃。

模块1.开发一个信息安全管理系统(SGSI)

1.1. 信息安全关键问题
1.1.1. 信息安全
- 1.1.1.1. 保密性
- 1.1.1.2. 整合
- 1.1.1.3. 可利用性
- 1.1.1.4. 信息安全措施

1.2. 信息安全管理体系
1.2.1. 信息安全管理模式
1.2.2. 实施SGSI的文件
1.2.3. SGSI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. 目标和范围
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. 一般信息安全系统的设计和实施
1.5.1. 一般信息安全系统的实施阶段
1.5.2. 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. 符合标准/规范的程度

1.7. 第二阶段:准备
1.7.1. 组织背景
1.7.2. 适用安全法规分析
1.7.3. 整个信息安全系统的范围
1.7.4. 一般信息安全系统政策
1.7.5. 总体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. 事件管理中的安全政策
1.10.1. 各个阶段
1.10.2. 事件的分类
1.10.3. 事件程序和事件管理

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. 资产 负债
2.2.2. 信息分类
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. 对易受攻击的业务流程的分析
2.3.2. 业务影响分析
2.3.3. 在业务影响方面对流程进行排序

2.4. 与人力资源有关的安全政策
2.4.1. 签约前
2.4.2. 签约期间
2.4.3. 终止或改变职位

2.5. 管理层面的安全政策
2.5.1. 信息安全的管理准则
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. 要求信息系统的安全
2.6.2. 开发和支持数据的安全
2.6.3. 测试数据

2.7. 与供应商的安全
2.7.1. 与供应商的IT安全
2.7.2. 与担保提供服务的管理
2.7.3. 供应链的安全

2.8. 运营安全
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. 活动和监测记录

2.9. 安全管理和法规
2.9.1. 遵守法律要求
2.9.2. 信息安全审查

2.10. 业务连续性管理中的安全
2.10.1. 信息安全的延续性
2.10.2. 冗余

模块3.计算机系统威胁分析的安全政策

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

3.2. 威胁管理的各个阶段
3.2.1. 识别
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. 分类和信息流
3.3.2. 分析脆弱的程序

3.4. 风险分类
3.4.1. 风险的类型
3.4.2. 威胁概率的计算
3.4.3. 剩余风险

3.5. 风险处理
3.5.1. 保障措施的实施
3.5.2. 转让或接管

3.6. 风险控制
3.6.1. 持续的风险管理过程
3.6.2. 实施安全衡量标准
3.6.3. 信息安全度量的战略模式

3.7. 威胁分析和监测的实用方法
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. 威胁的概率
3.9.3. 损害的程度

3.10. 危害分析中阶段和过程的设计
3.10.1. 确定组织的关键因素
3.10.2. 确定威胁和影响
3.10.3. 影响和风险分析
3.10.4. 方法

模块4.软件和硬件中安全策略的实际实施

4.1. 软件和硬件中安全策略的实际实施
4.1.1. 实施识别和授权
4.1.2. 识别技术的实施
4.1.3. 授权的技术措施

4.2. 识别和授权技术
4.2.1. 识别器和OTP
4.2.2. USB令牌或PKI智能卡
4.2.3. 机密防卫 ”钥匙
4.2.4. 有源RFID

4.3. 关于访问软件和系统的安全政策
4.3.1. 访问控制政策的实施
4.3.2. 通信访问政策的实施
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. 访问角色和功能的隔离
4.4.3. 系统中访问权限的实施

4.5. 对系统和应用程序的访问控制
4.5.1. 最低访问规则
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. 系统堡垒的CIS控制
4.7.1. 基本的CIS控制
4.7.2. 基本的CIS控制
4.7.3. 组织性的CIS控制

4.8. 运营安全
4.8.1. 对恶意代码的保护
4.8.2. 后备副本
4.8.3. 活动的记录和监测

4.9. 技术脆弱性的管理
4.9.1. 技术漏洞
4.9.2. 对技术脆弱性的管理
4.9.3. 软件安装的限制

4.10. 安全政策实践的实施
4.10.1. 逻辑上的漏洞
4.10.2. 防御政策的实施

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安置的标准

5.3. 安全事件响应
5.3.1. 信息收集程序
5.3.2. 入侵验证程序
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. 作为安全政策的取证分析
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. 对电子证据的分析
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. 活动集中化工具
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. 度量和指标

5.9. NIST SP800-61
5.9.1. 计算机安全事件响应能力
5.9.2. 事件处理
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. 事故应对行动指南

模块6.在公司实施实体和环境安全政策

6.1. 安全领域
6.1.1. 实体安全周界
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. 实物进入控制政策
6.2.2. 实物进入控制系统

6.3. 实物访问的脆弱性
6.3.1. 主要的物理漏洞
6.3.2. 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. 人脸识别
6.4.3. 虹膜和视网膜识别
6.4.4. 其他生理学生物识别系统

6.5. 行为生物识别系统
6.5.1. 签名识别
6.5.2. 书写者识别
6.5.3. 语音识别
6.5.4. 其他生物识别行为系统

6.6. 生物统计学风险管理
6.6.1. 生物识别系统的实施
6.6.2. 生物识别系统的脆弱性

6.7. 主机政策的实施
6.7.1. 布线配置和安全的安装
6.7.2. 设备管理
6.7.3. 设备在场所外的出口
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 (欧洲)
6.10.2. NERC CIP-005-5 (美国)
6.10.3. NERC CIP-014-2 (美国)

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模式
7.2.2. IPSEC 协议
7.2.3. TLS 协议

7.3. TLS 1.3协议
7.3.1. TLS过程的各个阶段1.3
7.3.2. 握手协议
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. 通讯中使用的加密算法
7.4.2. 密码套件
7.4.3. TLS 1.3允许的加密算法

7.5. 文摘功能
7.5.1. 文摘功能
7.5.2. MD6
7.5.3. SHA

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

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

7.8. SSH.安全外壳
7.8.1. SSH.安全胶囊
7.8.2. SSH的操作
7.8.3. SSH工具

7.9. 加密系统的审计
7.9.1. 完整性测试
7.9.2. 加密系统测试

7.10. 密码系统
7.10.1. 加密系统的漏洞
7.10.2. 密码保障措施

模块8.面对攻击时安全策略的实际实施

8.1. 系统黑客攻击
8.1.1. 风险和弱点
8.1.2. 对策

8.2. 服务中的DoS
8.2.1. 风险和弱点
8.2.2. 对策

8.3. 会话劫持
8.3.1. 劫持行为过程
8.3.2. 劫持行为的反措施

8.4. 对IDS,防火墙和蜜罐的规避
8.4.1. 规避技巧
8.4.2. 实施反措施

8.5. 黑客攻击网络服务器
8.5.1. 对网络服务器的攻击
8.5.2. 实施防御措施

8.6. 黑客攻击网络应用程序
8.6.1. 对网络应用程序的攻击
8.6.2. 实施防御措施

8.7. 黑客攻击无线网络
8.7.1. 无线网络的弱点
8.7.2. 实施防御措施

8.8. 黑客攻击移动平台
8.8.1. 移动平台的弱点
8.8.2. 实施反措施

8.9. Ramsonware(拉姆松)
8.9.1. Ramsonware软件造成的漏洞
8.9.2. 实施反措施

8.10. 社会工程
8.10.1. 社会工程的类型
8.10.2. 社会工程的对策

模块9.信息系统安全政策中的监测工具

9.1. 信息系统监测政策
9.1.1. 系统监测
9.1.2. 衡量标准度量衡
9.1.3. 衡量标准的类型

9.2. 系统中的审计和日志记录
9.2.1. 系统中的审计和日志
9.2.2. 窗口审计和日志记录
9.2.3. Linux上的审计和日志记录

9.3. SNMP协议简单网络管理协议
9.3.1. SNMP 协议
9.3.2. SNMP的操作
9.3.3. SNMP工具

9.4. 网络监控
9.4.1. 控制系统中的网络监控
9.4.2. 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的操作
9.5.3. 安装Nagios

9.6. Zabbix.网络监控系统
9.6.1. Zabbix.
9.6.2. Zabbix的运作
9.6.3. 安装Zabbix

9.7. Cacti.网络监控系统
9.7.1. Cacti.
9.7.2. Cacti 的运作
9.7.3. Cacti 的安装

9.8. 潘多拉.网络监控系统
9.8.1. 潘多拉.
9.8.2. Pandora的运作
9.8.3. Pandora多拉

9.9. SolarWinds. 网络监控系统
9.9.1. SolarWinds.
9.9.2. 操作SolarWinds
9.9.3. 安装SolarWinds

9.10. 监控条例
9.10.1. CIS对审计和记录的控制
9.10.2. NIST800-123(EE.UU)

模块10.实用的安全灾难恢复政策

10.1. DRP. 灾难恢复计划
10.1.1. 灾难恢复计划的目标
10.1.2. 灾难恢复计划的好处
10.1.3. 没有DRP和不保持更新的后果

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. 清点硬件,软件和服务
10.2.5. 对停工和数据丢失的容忍度
10.2.6. 确定所需的特定类型的DRP
10.2.7. 实施培训,认识和沟通计划

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

10.4. DRP（灾难恢复）战略的设计
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. 连续性的验证和评价

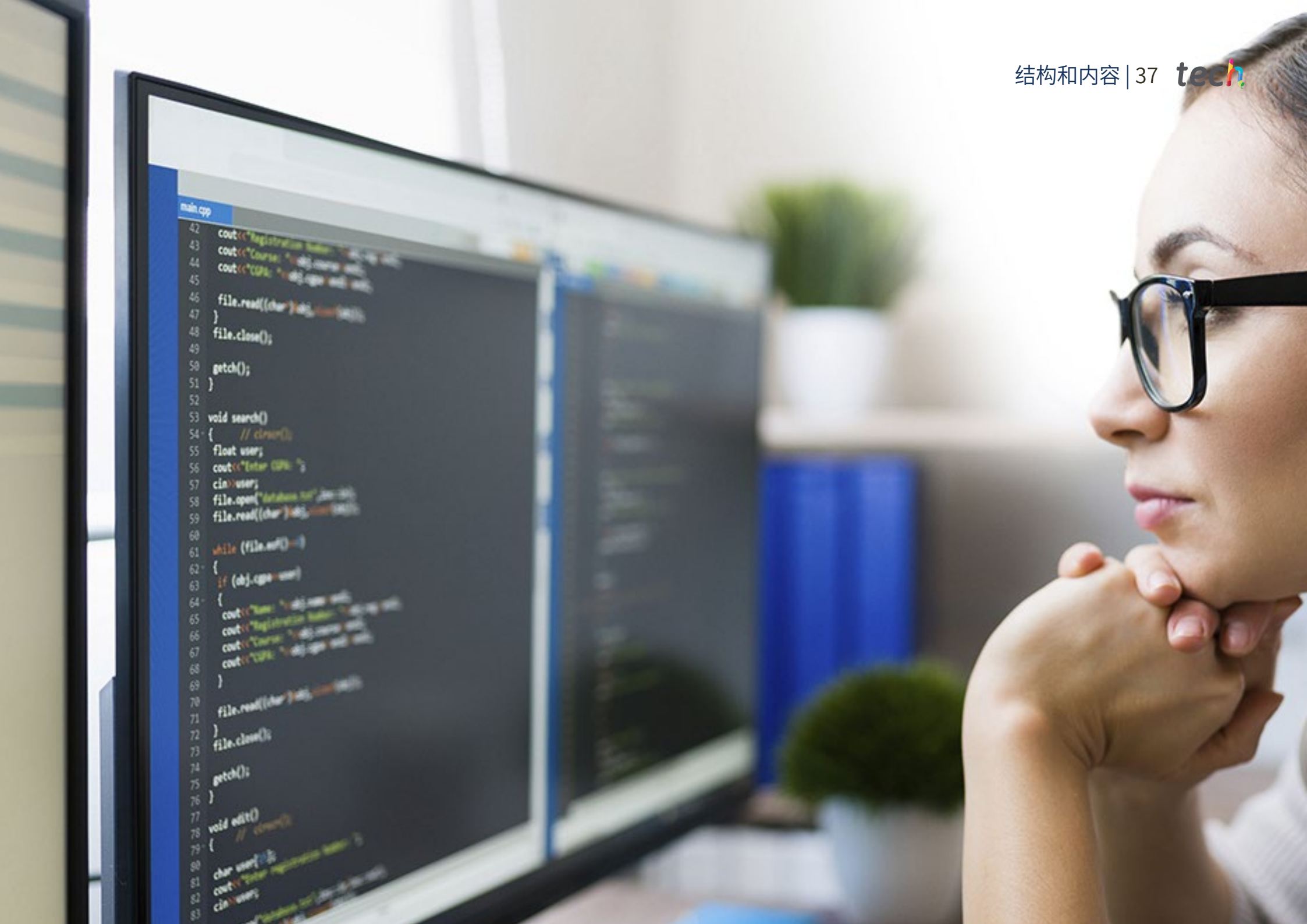
10.6. BCP（业务连续性计划）的范围
10.6.1. 确定最关键的流程
10.6.2. 基于资产的方法
10.6.3. 过程方法

10.7. 实施安全的商业流程
10.7.1. 优先活动（AP）
10.7.2. 理想恢复时间（TRI）
10.7.3. 生存策略

10.8. 组织的分析
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. 应变反应
10.9.1. 危机计划
10.9.2. 运行环境恢复计划
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


main.cpp

07

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”

TECH商学院使用案例研究来确定所有内容的背景

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”

该课程使你准备好在不确定的环境中面对商业挑战，使你的企业获得成功。

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。

一种创新并不同的学习方法

该技术课程是一个密集的培训课程，从头开始创建，为国内和国际最高水平的管理人员提供挑战和商业决策。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基础的技术，确保遵循最新的经济，社会和商业现实。

> 你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”

在世界顶级商学院存在的时间里，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临的问题，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

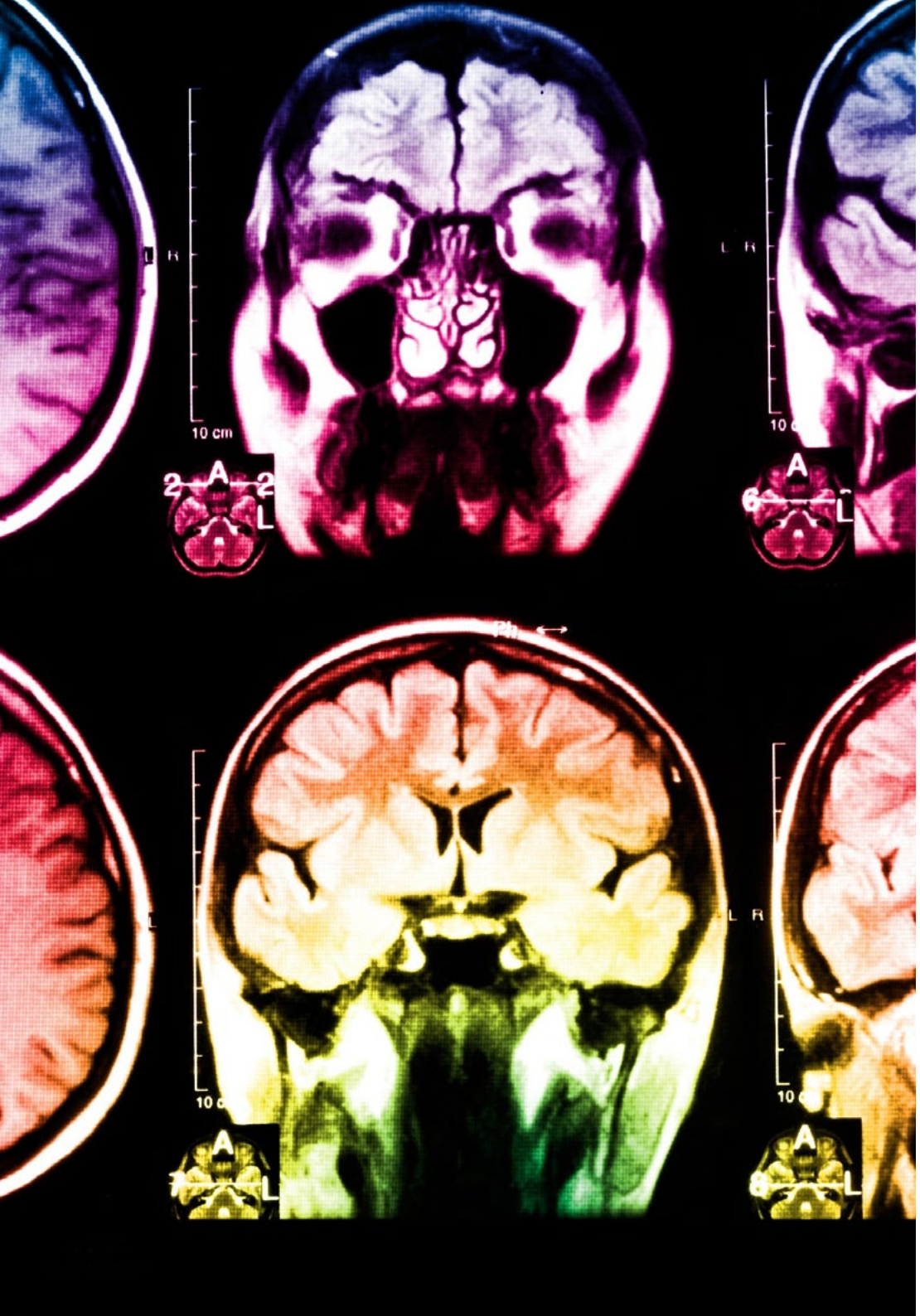
TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合，在每节课中结合了个不同的教学元素。

我们用最好的100%在线教学方法加强案例研究:再学习。

> 我们的在线系统将允许你组织你的时间和学习节奏，使其适应你的时间表。你将能够从任何有互联网连接的固定或移动设备上获取容。

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。

我们的商学院是唯一获准采用这种成功方法的西班牙语学校。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。

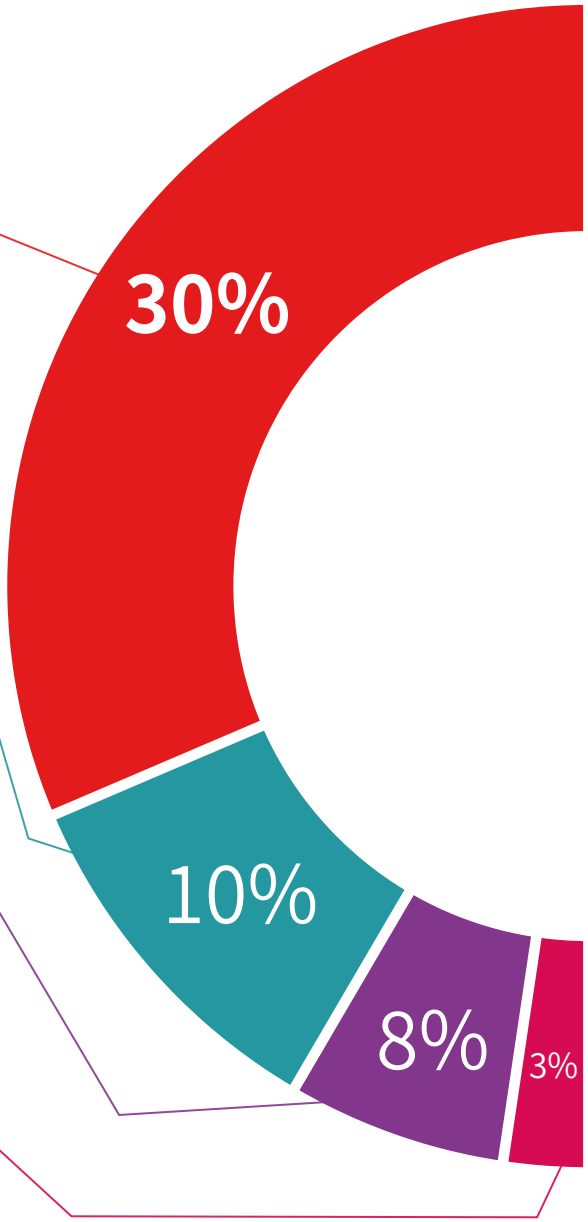
向专家学习可以加强知识和记忆，并为未来的困难决策建立信心。

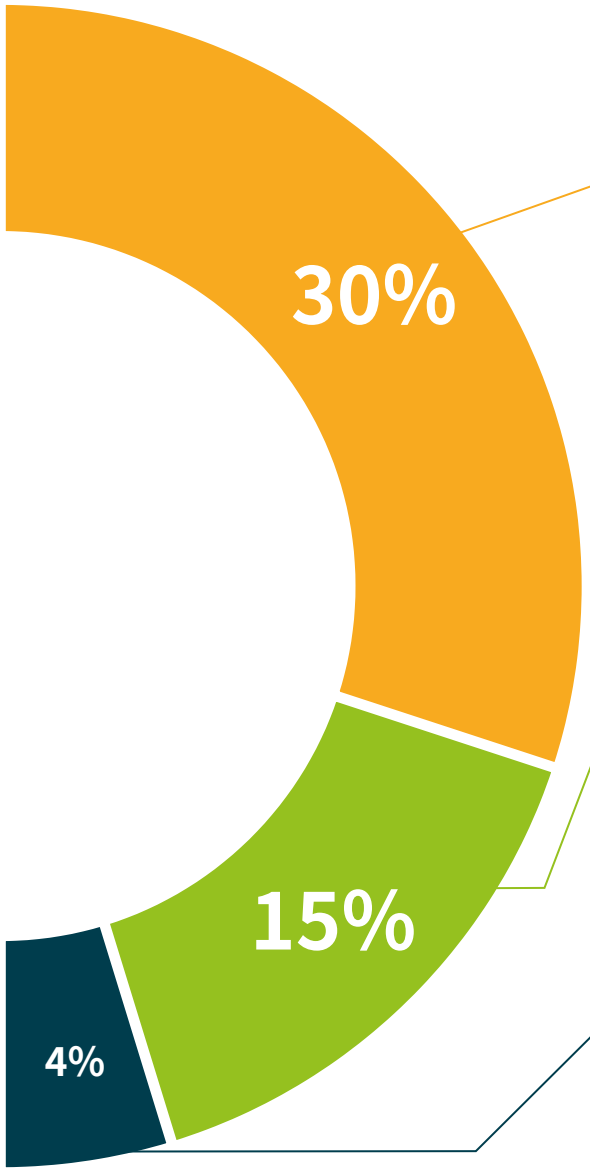
管理技能实习

他们将在每个学科领域开展具体的管理能力发展活动。获得和培训高级管理人员在我们所处的全球化框架内所需的技能和能力的做法和新情况。

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。由国际上最好的高级管理专家介绍，分析和辅导的案例。

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。

08

我们的学生简介

商学院校级硕士的对象是大学毕业生,毕业生和以前在社会和法律科学,行政和经济领域完成过以下任何一个学位的毕业生。

该课程的目的是巩固学生对任何商业实体的财务会计的基本和高级知识。科方法。

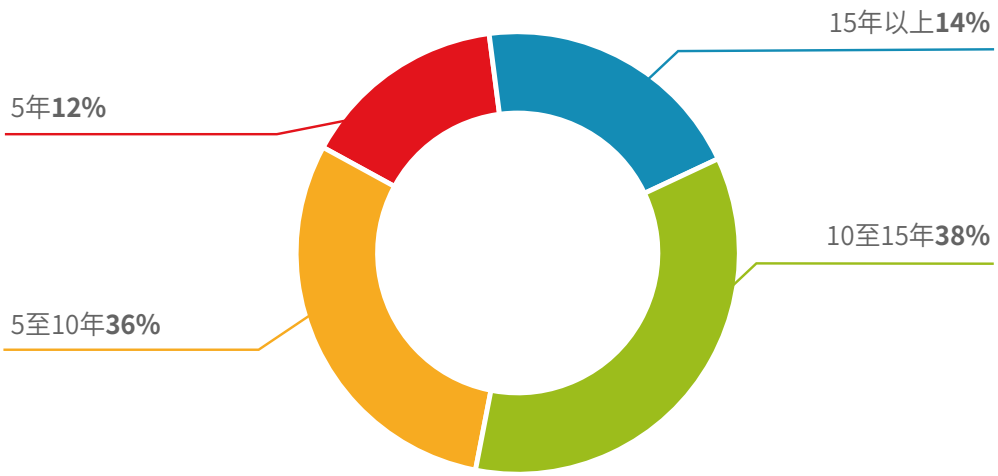
作为任何领域的大学毕业生，在网络安全政策管理领域有两年工作经验的专业人士也可以攻读该商学院校级硕士。

如果你希望以高质量的知识来促进你的职业生涯，并以当前最现实的网络安全为基础，现在就报名参加这个课程”

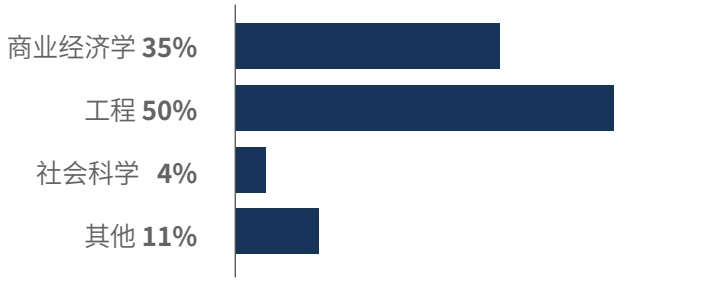
平均年龄

35岁至**45**岁之间

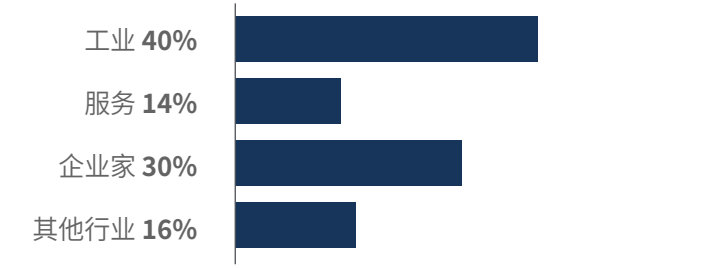
经验年限



培训



学术概况



地域分布

Gabriel Gutiérrez Gómez

网络安全主管

“在我们的组织遭受严重的计算机攻击后，我们更加重视保护我们的数据库，并专门成立了一个小部门。感谢这个项目，我能够领导这项工作，设计和实施我们今天仍然使用的网络安全政策”

09

课程管理

为了使所有的教学内容达到尽可能高的质量，TECH选择了一批在网络安全所涉及的不同领域的专家教师。因此，管理者可以获得由在网络安全政策管理方面具有丰富经验的专业人士编写的教学大纲，他们以其独特的实践眼光为所涉及的每个主题贡献了所有理论。

你将得到具有高级管理和复杂的IT安全管理经验的教学人员的支持，有专门的信息系统维护,取证分析和劫持等科目”

地址

Fernández Sapena, Sonia 女士

- 马德里赫塔菲的国家计算机和电信参考中心的计算机安全和道德黑客培训师
- 认证的电子理事会讲师
- 获得以下认证的培训师：EXIN 道德 黑客基金会 以及 EXIN 网络和 IT 安全基金会。马德里
- 获得以下专业证书的CAM专家认证培训师：计算机安全（IFCT0190），语音和数据网络管理（IFCM0310），部门网络管理（IFCT0410），电信网络警报管理（IFCM0410），语音和数据网络运营商（IFCM0110）和互联网服务管理（IFCT0509）
- 巴利阿里群岛大学外部合作者CSO/SSA（首席安全官/高级安全架构师）
- 马德里毕业于阿尔卡拉德埃纳雷斯大学的生物学专业
- DevOps 硕士：Docker 和 KubernetesCas-培训
- 微软 Azure 安全技术。E 理事会

教师

Solana Villarias, Fabián 先生

- 信息技术顾问
- Investigación, Planificación y Desarrollo, S.A.的调查服务的开发者和管理者
- 伊比利亚金融软件公司的金融市场和IT系统维护专家
- 英德拉的网站开发和可访问性专家
- 卡斯蒂利亚-拉曼恰大学计算机科学工程学士
- 威尔士大学/CESINE的高等系统工程学位

López, Rosa María 女士

- 管理信息专家
- Linux专业学院的讲师
- Incibe黑客学院的合作者
- Teamciberhack的网络安全人才队长
- Integra2Transportes的行政,会计和财务经理
- 在Cardenal Marcelo Espínola教育中心担任采购资源的行政助理
- 网络安全和道德黑客的高级技术员
- Ciberpatrulla的成员

Oropesiano Carrizosa, Francisco 先生

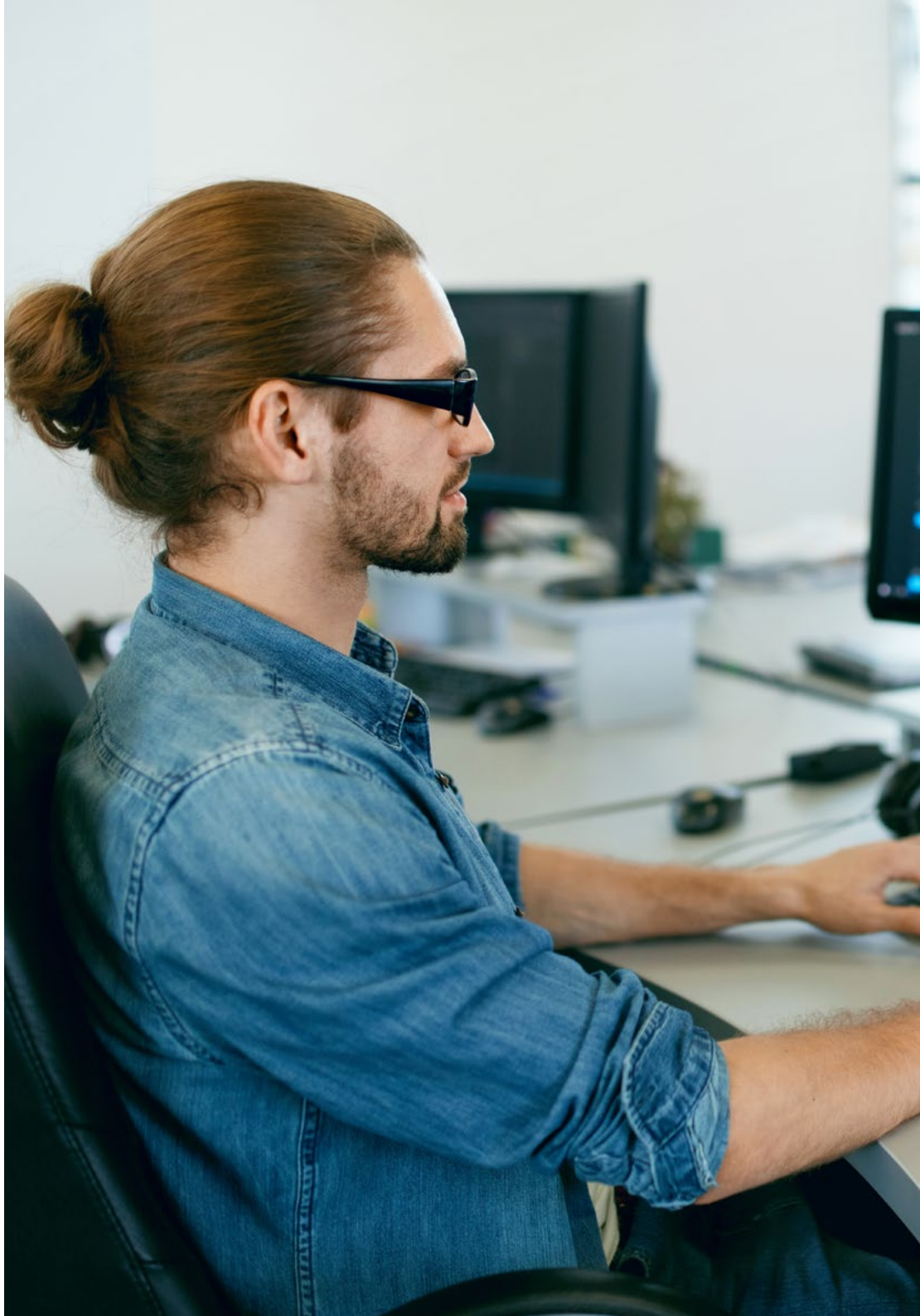
- 计算机工程师
- 在Cas-Training工作的微机,网络和安全技术员
- 在Fersa Reparaciones的网络服务,CMS,电子商务,UI和UX开发人员
- 在Oropesia Web & Network担任网络服务,内容,邮件和DNS管理员
- 在Xarxa Sakai Projectes担任图形和网络应用程序设计师
- 阿尔卡拉-德-埃纳雷斯大学计算机系统专业毕业
- DevOps硕士: 网络商业中心的Docker和Kubernetes课程
- 巴利阿里群岛大学网络技术人员和计算机安全
- 马德里理工大学平面设计专家

Ortega López, Florencio 先生

- SIA集团安全顾问(身份管理)
- 作为独立专业人士的ICT和安全顾问
- IT部门培训教授
- Alcaláde Henares大学工业技术工程硕士
- 联合教师硕士
- IDE-CESEM工商管理硕士
- IDE-CESEM信息技术方向和管理硕士
- ISACA认证的信息安全管理(CISM)

Peralta Alonso, Jon 博士

- 高级顾问-数据保护和网络安全。Altia
- 律师/法律顾问Arriaga Associates 法律和经济咨询，S.L.
- 法律顾问/实习生。专业办公室：Oscar Padura
- 法学学位。巴斯克地区公立大学
- 数据保护代表的硕士EIS创新学校
- 法学硕士巴斯克地区公立大学
- 民事诉讼实践专业硕士伊莎贝尔一世国际卡斯蒂利亚大学
- 个人数据保护,网络安全和信息通信技术法硕士的



TECH精心挑选了这个课程的教学团队，以便你能从当今最好的专家那里学到东西”

10

对你的职业生涯的影响

TECH意识到管理人员必须努力获得这些特征的学位，因此特别努力确保所提供的所有内容和教学材料符合最严格的质量标准。因此，可以访问的多媒体图书馆是网络安全领域的一个特殊参考，甚至可以完全下载，以便在学位结束后继续使用。

您将获得您所寻求的经济和专业预测，这要归功于一个致力于将您带到网络安全政策管理中心的教学和技术团队的持续支持”

你准备好迈出这一步了吗？卓越的职业提升在等着你

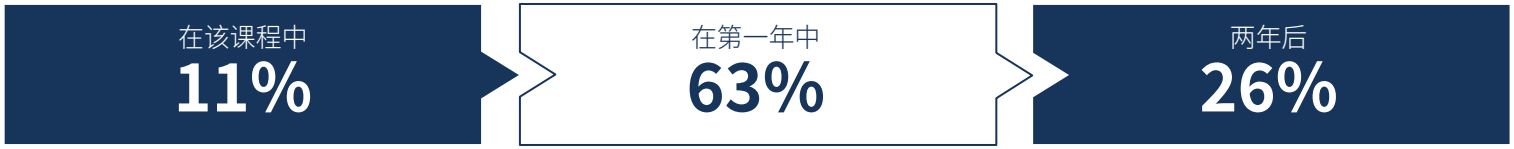
TECH的企业的网络安全政策管理商学院校级硕士，为你在美食领域面对挑战和商业决策做好准备。其主要目标是促进你的个人和职业帮助你获得成功。

如果你想提高自己，在专业水平上实现积极的变化，并与最好的人交流，这里就是你的地方。

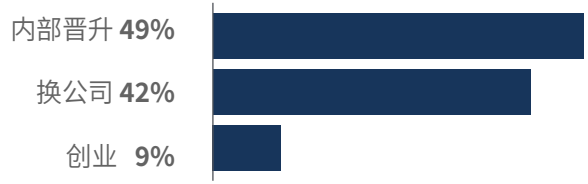
多亏了TECH的教学方法，您将在比您想象的更短的时间内实现您所追求的工作改进。

现在就注册这个商学院校级硕士，不要再等待你周围的积极变化了。

改变的时候到



改变的类型



工资提高

完成这个课程后，我们学生的工资会增长超过**25.22%**。

11

对贵公司的好处

企业的网络安全政策管理商学院校级硕士,通过培训高级领导人,帮助最大限度地发挥组织的人才潜力

此外,加入该高级专科文凭是一个独特的机会,可以进入一个强大的联系网络,在其中寻找未来的专业合作伙伴,客户或供应商。

网络威胁是各种类型和规模的公司面临的最大脆弱性之一。专注于未来预测最大的领域”

培养和留住公司的人才是最好的长期投资。

01

人才和智力资本的增长

该专业人员将为公司带来新的概念,战略和观点,可以为组织带来相关的变化。

02

留住高潜力的管理人员,避免人才流失

这个计划加强了公司和经理人之间的联系,并为公司内部的职业发展开辟了新的途径。

03

培养变革的推动者

你将能够在不确定和危机的时候做出决定,帮助组织克服障碍。

04

增加国际扩张的可能性

由于这一计划,该公司将与世界经济的主要市场接触。

05

开发自己的项目

经理可以在一个真实的项目上工作，或在其公司的研发或业务发展领域开发新项目。

06

提高竞争力

公司数据科学技术管理商学院校级硕士将使学生具备接受新挑战的技能，从而促进组织的发展。

12

学位

企业的网络安全政策管理专科文凭课程除了保证最严格和最新的培训外，还可以获得由TECH科技大学颁发的专科文凭学位证书。

顺利完成该课程并获得大学学位，无需旅行或文书工作的麻烦”

这个**企业的网络安全政策管理大学课程**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：**企业的网络安全政策管理大学课程**

官方学时：**150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

商学院校级硕士

企业的网络安全政策管理

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


商学院校级硕士企业的网络安全政策管理

教学大纲概况

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

学期	学科	小时	性质
1°	开发一个信息安全管理系统 (SGSI)	150	必修
1°	信息安全政策的组织方面	150	必修
1°	计算机系统威胁分析的安全政策	150	必修
1°	软件和硬件中安全策略的实际实施	150	必修
1°	安全事件管理政策	150	必修
1°	在公司实施实体和环境安全政策	150	必修
1°	企业中的安全通信政策	150	必修
1°	面对攻击时安全策略的实际实施	150	必修
1°	信息系统安全政策中的	150	必修
1°	实用的安全灾难恢复政策	150	必修

言语和语言治疗的基础]

Tere Guevara Navarro女士
校长

tech 科学技术大学

tech 科学技术大学

商学院校级硕士
企业的网络安全政策管理

- 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**

商学院校级硕士
企业的网络安全政策管理

tech 科学技术大学