Curso de Especialização

Administração da Segurança das Tecnologias da Informação

tech universidade tecnológica

tech universidade tecnológica

Curso de Especialização

Administração da Segurança das Tecnologias da Informação

- Modalidade: **Online**
- Duração: **6 meses**
- Certificação: **TECH Universidade Tecnológica**
- Créditos: **18 ECTS**
- Horário: **Ao seu próprio ritmo**
- Exames: **Online**

Acesso ao site: **www.techtitute.com/pt/informatica/curso-especializacao/curso-especializacao-administracao-seguranca-tecnologias-informacao**

Índice

01

Apresentação

A integração das tecnologias da informação em muitas empresas teve um efeito colateral: os riscos de segurança informática aumentaram. Agora, as empresas precisam de estar conscientes dos vários ataques e vulnerabilidades que podem afetar o seu bom funcionamento e os seus serviços. Por isso, é essencial ter um especialista na empresa que seja responsável pela gestão da segurança em torno destas tecnologias. Este Curso de Especialização oferece ao profissional a oportunidade de conhecer os métodos de proteção informática mais desenvolvidos nesta área, uma vez que lhe proporcionará um conhecimento aprofundado de aspetos como a avaliação de riscos com base em parâmetros de negócio, a gestão de identidades e acessos ou os testes de intrusão.

Cada vez mais são as empresas que necessitam de especialistas em administração de segurança aplicada às tecnologias da informação. Este Curso de Especialização permitir-lhe-á evoluir profissionalmente, aprofundando questões como o Plano de Continuidade do Negócio associado à segurança"

É um facto: quase não existem empresas que não utilizem ferramentas digitais e informáticas nos seus processos internos. Atividades e operações como a identificação dos trabalhadores, os sistemas logísticos ou o contacto com fornecedores e clientes são agora realizados principalmente através das tecnologias da informação. No entanto, estas tecnologias devem ser objeto de design e controlo adequados, uma vez que podem ser exploradas para obter dados ou violar o acesso a aspetos sensíveis da empresa.

Por este motivo, o especialista em administração de segurança é um cargo cada vez mais procurado e não pode ser substituído por qualquer informático. São necessários conhecimentos altamente atualizados que tenham em conta os últimos desenvolvimentos em matéria de cibersegurança. Assim, este Curso de Especialização foi desenvolvido para dar a conhecer ao profissional os últimos desenvolvimentos neste domínio, aprofundando questões como as auditorias de segurança, a segurança dos equipamentos terminais, ou a resposta mais eficaz a diferentes incidentes.

Este Curso de Especialização é também desenvolvido num formato 100% online que se adapta às circunstâncias do profissional, permitindo-lhe estudar quando, onde e como quiser. Contará também com um corpo docente de grande prestígio no domínio da cibersegurança que será apoiado por numerosos recursos multimédia para tornar o processo de aprendizagem confortável, rápido e eficaz.

Este **Curso de Especialização em Administração da Segurança das Tecnologias da Informação** conta com o conteúdo educativo mais completo e atualizado do mercado. As suas principais características são:

- O desenvolvimento de casos práticos apresentados por especialistas em Informática Cibersegurança
- O conteúdo gráfico, esquemático e eminentemente prático fornece informações científicas e práticas sobre as disciplinas que são essenciais para a prática profissional
- Exercícios práticos em que o processo de autoavaliação pode ser utilizado para melhorar a aprendizagem
- A sua ênfase especial em metodologias inovadoras
- Palestras teóricas, perguntas ao especialista, fóruns de discussão sobre questões controversas e atividades de reflexão individual.
- A disponibilidade de acesso ao conteúdo a partir de qualquer dispositivo fixo ou portátil com ligação à Internet

Este Curso de Especialização permitir-lhe-á aprofundar aspetos como o ciclo de vida de um Plano de Continuidade de Negócio ou a gestão de vulnerabilidades"

A TECH coloca à sua disposição os melhores recursos multimédia: estudos de casos, atividades teórico-práticas, vídeos, resumos interativos, etc. Tudo para que o processo de aprendizagem seja ágil e possa tirar o máximo partido de cada minuto investido"

Será capaz de responder adequadamente a todo o tipo de ameaças de cibersegurança. Matricule-se e torne-se num grande especialista.

Estudar ao seu próprio ritmo, sem interrupções nem horários fixos: o método de ensino da TECH é muito prático.

O corpo docente do Curso de Especialização inclui profissionais do setor que trazem a sua experiência profissional para esta capacitação, para além de especialistas reconhecidos de sociedades de referência e universidades de prestígio.

Graças ao seu conteúdo multimédia, desenvolvido com a mais recente tecnologia educativa, o profissional terá acesso a uma aprendizagem situada e contextual, isto é, um ambiente de simulação que proporcionará uma educação imersiva, programada para praticar em situações reais.

A conceção desta qualificação centra-se na Aprendizagem Baseada em Problemas, através da qual o especialista deve tentar resolver as diferentes situações da prática profissional que surgem ao longo do Curso de Especialização. Para tal, contará com a ajuda de um sistema inovador de vídeo interativo desenvolvido por especialistas reconhecidos.

02

Objetivos

Tendo em conta a crescente complexidade do domínio da cibersegurança, o principal objetivo deste Curso de Especialização em Administração da Segurança das Tecnologias da Informação é aproximar os profissionais das novidades mais importantes neste domínio. Assim, poderá tornar-se um grande especialista neste domínio, podendo trabalhar na área da gestão e direção da cibersegurança de empresas de todos os tipos de setores.

A TECH ajuda-o a atingir os seus objetivos graças a este Curso de Especialização, com o qual poderá candidatar-se a importantes cargos profissionais nas mais importantes empresas nacionais e internacionais"

Objetivos gerais

- Desenvolver um Sistema de Gestão de Segurança da Informação(SGSI)
- Identificar os elementos-chaves que conformam um SGSI
- Avaliar os diferentes modelos de arquitetura de segurança para estabelecer o modelo mais apropriado para a organização
- Identificar os quadros regulamentares aplicáveis e as bases reguladoras dos mesmos
- Analisar a estrutura organizacional e funcional de uma área de segurança da informação (o departamento do CISO)
- Estabelecer um programa de auditoria que satisfaça as necessidades de autoavaliação da organização em matéria de cibersegurança
- Desenvolver um programa de análise e controlo de vulnerabilidades e um plano de resposta a incidentes de cibersegurança
- Determinar os elementos básicos de um Plano de Continuidade de Negócio (PCN) utilizando como base as orientações da norma ISO-22301
- Examinar os riscos decorrentes da inexistência de um Plano de Continuidade de Negócio (PCN)
- Analisar os critérios de sucesso de um PCN e a sua integração na gestão de riscos global de uma empresa
- Definir as fases de implementação de um Plano de Continuidade de Negócio

Objetivos específicos

Módulo 1 Arquiteturas e modelos de segurança da informação

- Alinhar o Plano Diretor de Segurança com os objetivos estratégicos da organização
- Estabelecer um quadro contínuo de gestão de riscos como parte integrante do Plano Diretor de Segurança
- Determinar os indicadores apropriados para monitorizar a implementação do SGSI
- Estabelecer uma estratégia de segurança baseada em políticas
- Analisar os objetivos e procedimentos associados ao plano de sensibilização dos empregados, fornecedores e sócios
- Identificar, dentro do quadro regulamentar, os regulamentos, certificações e leis aplicáveis a cada organização
- Desenvolver os elementos fundamentais exigidos pela norma ISO 27001:2013
- Implementar um modelo de gestão da privacidade em conformidade com o regulamento europeu GDPR/RGPD

Módulo 2 Gestão da Segurança IT

- Identificar as diferentes estruturas que pode ter uma área de segurança da informação
- Desenvolver um modelo de segurança baseado em três linhas de defesa
- Apresentar os diferentes comités periódicos e extraordinários em que está envolvida a área de cibersegurança
- Identificar as ferramentas tecnológicas que apoiam as principais funções da equipa de operações de segurança (SOC)
- Avaliar as medidas de controlo da vulnerabilidade adequadas a cada cenário
- Desenvolver o quadro de operações de segurança com base em NIST CSF
- Especificar o âmbito dos diferentes tipos de auditorias (*Red Team, Pentesting, Bug Bounty*,etc.)
- Propor as atividades a serem realizadas após um incidente de segurança
- Configurar um centro de comando de segurança da informação que englobe todos os atores relevantes (autoridades, clientes, fornecedores, etc.)

Módulo 3 Plano de continuidade do negócio associado à segurança

- Apresentar os elementos-chave de cada fase e analisar as caraterísticas do Plano de Continuidade de Negócio (PCN)
- Fundamentar a necessidade de um Plano de Continuidade para o Negócio
- Determinar os mapas de sucesso e de risco para cada fase do Plano de Continuidade de Negócio
- Especificar como é estabelecido um Plano de Ação para a implementação
- Avaliar a integridade de um Plano de Continuidade de Negócios (PCN)
- Desenvolver um plano para a implementação bem sucedida de umo Plano de Continuidade de Negócio

Será o maior especialista em segurança aplicada às tecnologias da informação no seu meio" Não espere mais: inscreva-se agora"

03

Direção do curso

Ter à sua disposição os maiores especialistas mundiais em gestão da segurança das TI é uma grande oportunidade para o profissional. E é exatamente isso que este Curso de Especialização oferece, com um corpo docente constituído por engenheiros e informáticos de prestígio, que fornecerão ao estudante as técnicas e os procedimentos mais evoluídos para garantir a adequada segurança interna de uma empresa.

Contactará com os maiores especialistas em cibersegurança, que partilharão consigo todas as ferramentas para trabalhar com a maior competência nesta área"

Direção

Sr. Martín Olalla Bonal

- Client Technical Specialist Blockchain na IBM
- Arquiteto *Blockchain*
- Arquiteto de Infraestruturas na Banca
- Gestão de projetos e implementação de soluções
- Técnico em Eletrónica Digital
- Docente: Formação *Hyperledger Fabric* a empresas
- Docente: Formação *Blockchain* indicada para negócios em empresas

Professores

Dr. Juan Luis Gozalo Fernández

- Engenheiro Informático
- Professor Associado em DevOps e em Blockchain em UNIR
- Ex-diretor Blockchain DevOps em Alastria
- Diretor Desenvolvimento Aplicação Móvel Tinkerlink em Cronos Telecom
- Diretor Informático em Banco Santander
- Diretor Tecnologia Gestão de Serviço IT em Barclays Bank Espanha
- Licenciado em Engenharia Superior Informático pela Universidade Nacional de Educação à Distância (UNED)

Dr. Mario Embid Ruiz

- Advogado especialista em Direitos TIC e proteção de dados
- Responsabilidade legal da Branddocs, SL Empresa Tecnológica de Soluções de Confiança
- Mestrado em Direito e Administração de Empresas pela Universidade Rey Juan Carlos
- Mestrado em Direito das Novas Tecnologias, Internet e Audiovisual pelo Centro de Estudos Universitários Villanueva y Cremades & Calvo Sotelo

Dr. Juan Manuel Rodrigo Estébanez

- Fundador de ISMET TECH S.L
- Licenciatura em Engenharia pela Universidade de Valladolid
- Mestrado e Sistemas de Gestão Integrados pela CFE-CEU
- ISO, 27001 Lead Auditor (IMQ)
- ISO, 27001 Lead Implementor (IMQ)
- NATO Standards HPS (OTAN)

04

Estrutura e conteúdo

O plano de estudos deste Curso de Especialização em Administração da Segurança das Tecnologias da Informação está organizado em três módulos que se desenrolam ao longo de 450 horas de aprendizagem. Nesse período, o profissional aprofundará aspetos relevantes deste setor como as análises forenses, os modelos de segurança da informação, o quadro normativo aplicável a esta área ou a configuração de regras de segurança de rede, entre muitas outras questões.

Terá à sua disposição o conteúdo mais completo, apresentado através de recursos didáticos ao quais poderá aceder 24 horas por dia"

Módulo 1. Arquiteturas e modelos de segurança da informação

1.1. Arquitetura de segurança da informação
- 1.1.1. SGSI/PDS
- 1.1.2. Alienação estratégica
- 1.1.3. Gestão do risco
- 1.1.4. Medição de desempenho

1.2. Modelos de segurança da informação
- 1.2.1. Baseados em políticas de segurança
- 1.2.2. Baseados em ferramentas de proteção
- 1.2.3. Baseados em equipas de trabalho

1.3. Modelo de segurança. Componentes-chave
- 1.3.1. Identificação de riscos
- 1.3.2. Definição de controlos
- 1.3.3. Avaliação contínua de níveis de risco
- 1.3.4. Plano de sensibilização de funcionários, fornecedores, sócios, etc.

1.4. Processo de gestão de riscos
- 1.4.1. Identificação de ativos
- 1.4.2. Identificação de ameaças
- 1.4.3. Avaliação de risco
- 1.4.4. Priorização de controlos
- 1.4.5. Reavaliação e risco residual

1.5. Processos de negócio e segurança da informação
- 1.5.1. Processos empresariais
- 1.5.2. Avaliação de risco com base em parâmetros de negócio
- 1.5.3. Análise do impacto no negócio
- 1.5.4. As operações de negócio e a segurança da informação

1.6. Processo de melhoria contínua
- 1.6.1. O ciclo de Deming
  - 1.6.1.1. Planificar
  - 1.6.1.2. Fazer
  - 1.6.1.3. Verificar
  - 1.6.1.4. Agir

1.7. Arquiteturas de segurança
- 1.7.1. Seleção e homogeneização de tecnologias
- 1.7.2. Gestão de identidades. Autenticação
- 1.7.3. Gestão de acessos Autorização
- 1.7.4. Segurança de infraestrutura de rede
- 1.7.5. Tecnologias e soluções de encriptação
- 1.7.6. Segurança de Equipas Terminais (EDR)

1.8. O quadro normativo
- 1.8.1. Normativas setoriais
- 1.8.2. Certificações
- 1.8.3. Legislações

1.9. A Norma ISO 27001
- 1.9.1. Implementação
- 1.9.2. Certificação
- 1.9.3. Auditorias e testes de intrusão
- 1.9.4. Gestão contínua do risco
- 1.9.5. Classificação da informação

1.10. Legislação sobre privacidade. Regulamento Geral de Proteção de Dados - RGPD (GDPR - General Data Protection Regulation)
- 1.10.1. Alcance do Regulamento Geral de Proteção de Dados (RGPD)
- 1.10.2. Dados pessoais
- 1.10.3. Papéis no tratamento de dados pessoais
- 1.10.4. Direitos ARCO
- 1.10.5. O DPO. Funções

Módulo 2. Gestão da Segurança IT

2.1. Gestão da Segurança
- 2.1.1. Operações de segurança
- 2.1.2. Aspeto legal e regulamentar
- 2.1.3. Habilitação do negócio
- 2.1.4. Gestão de risco
- 2.1.5. Gestão de identidades e acessos

2.2. Estrutura da área de segurança. O escritório do CISO
- 2.2.1. Estrutura organizativa. Posição do CISO (Chief Information Security Officer) na estrutura
- 2.2.2. As linhas de defesa
- 2.2.3. Organigrama do escritório do CISO
- 2.2.4. Gestão orçamental

2.3. Governo de segurança
- 2.3.1. Comité de segurança
- 2.3.2. Comité de monitorização de riscos
- 2.3.3. Comité de auditoria
- 2.3.4. Comité de crise

2.4. Governo de segurança. Funções
- 2.4.1. Políticas e normas
- 2.4.2. Plano Diretor de segurança
- 2.4.3. Painel de instrumentos
- 2.4.4. Sensibilização e formação
- 2.4.5. Segurança na cadeia de abastecimento

2.5. Operações de segurança
- 2.5.1. Gestão de identidades e acessos
- 2.5.2. Configuração de regras de segurança de rede. Firewalls
- 2.5.3. Gestão de plataformas IDS/IPS
- 2.5.4. Análise de vulnerabilidades

2.6. Quadro de trabalho de Cibersegurança NIST CSF
- 2.6.1. Metodologia NIST
  - 2.6.1.1. Identificar
  - 2.6.1.2. Proteger
  - 2.6.1.3. Detetar
  - 2.6.1.4. Responder
  - 2.6.1.5. Recuperar

2.7. Centro de Operações de Segurança (SOC). Funções
- 2.7.1. Proteção *Red Team, Pentesting, Threat Intelligence*
- 2.7.2. Deteção SIEM, *User Behavior Analytics, Fraud Prevention*
- 2.7.3. Resposta

2.8. Auditoria de segurança
- 2.8.1. Teste de intrusão
- 2.8.2. Exercícios *Red Team*
- 2.8.3. Auditorias de código-fonte. Desenvolvimento seguro
- 2.8.4. Segurança de componentes (*Software Supply Chain*)
- 2.8.5. Análise forense

2.9. Resposta a incidentes
- 2.9.1. Preparação
- 2.9.2. Deteção, análise e notificação
- 2.9.3. Contenção, erradicação e recuperação
- 2.9.4. Atividades pós-incidente
  - 2.9.4.1. Retenção de evidências
  - 2.9.4.2. Análise forense
  - 2.9.4.3. Gestão de brechas
- 2.9.5. Guias oficiais de gestão de ciberincidentes

2.10. Gestão de vulnerabilidades
- 2.10.1. Análise de vulnerabilidades
- 2.10.2. Avaliação de vulnerabilidade
- 2.10.3. Base de sistemas
- 2.10.4. Vulnerabilidade de dia 0. *Zero-Day*

Módulo 3. Plano de continuidade do negócio associado à segurança

3.1. Planos de Continuidade de Negócio
- 3.1.1. Os Planos de Continuidade de Negócio (PCN)
- 3.1.2. Plano de Continuidade de Negócio (PCN). Questões-chave
- 3.1.3. Plano de Continuidade de Negócio (PCN) para a avaliação da empresa

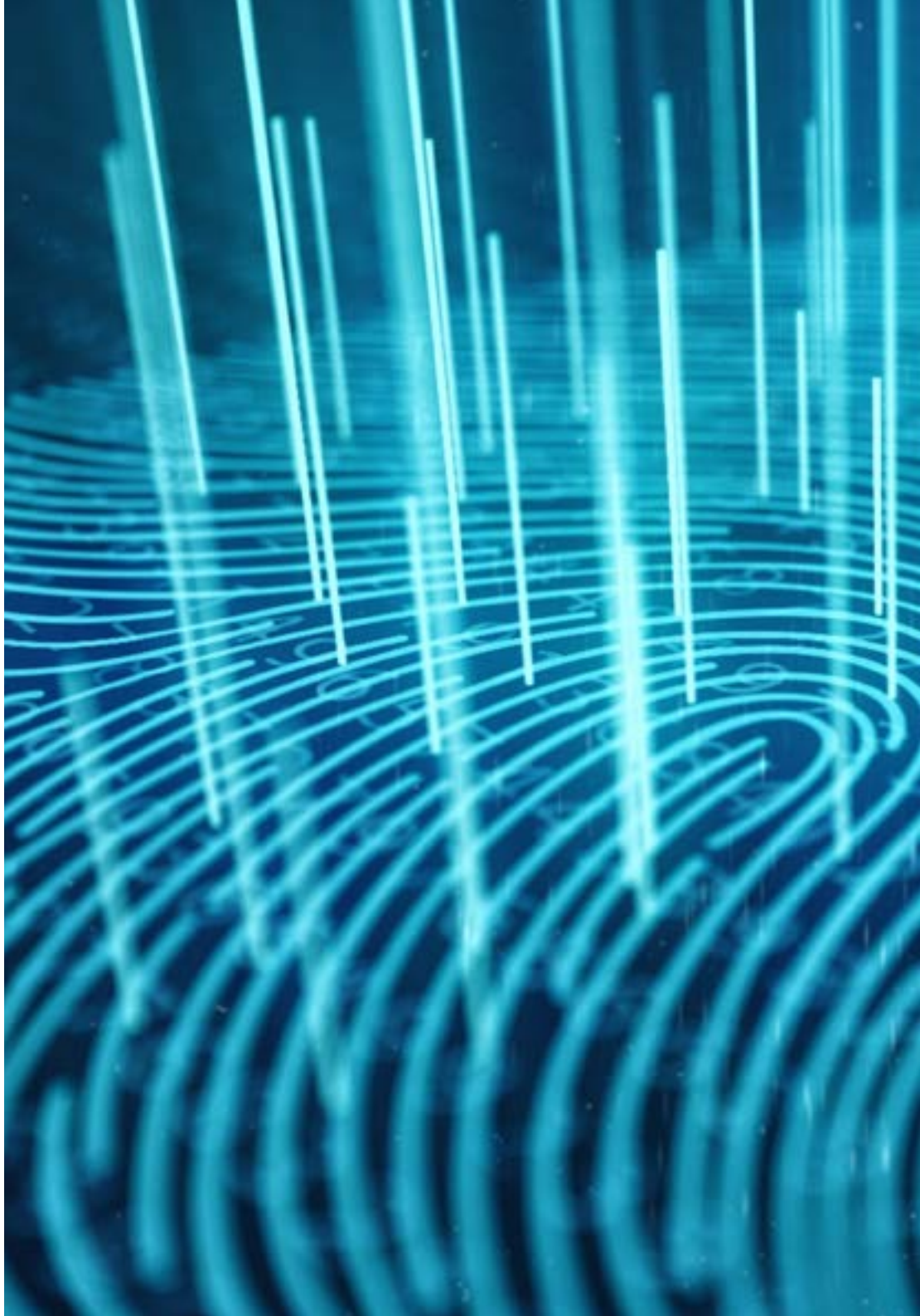
3.2. Métricas num Plano de Continuidade de Negócio (PCN)
- 3.2.1. *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO)
- 3.2.2. Tempo Máximo Tolerável (MTD)
- 3.2.3. Níveis Mínimos de Recuperação (ROL)
- 3.2.4. Ponto de Recuperação Objetivo (RPO)

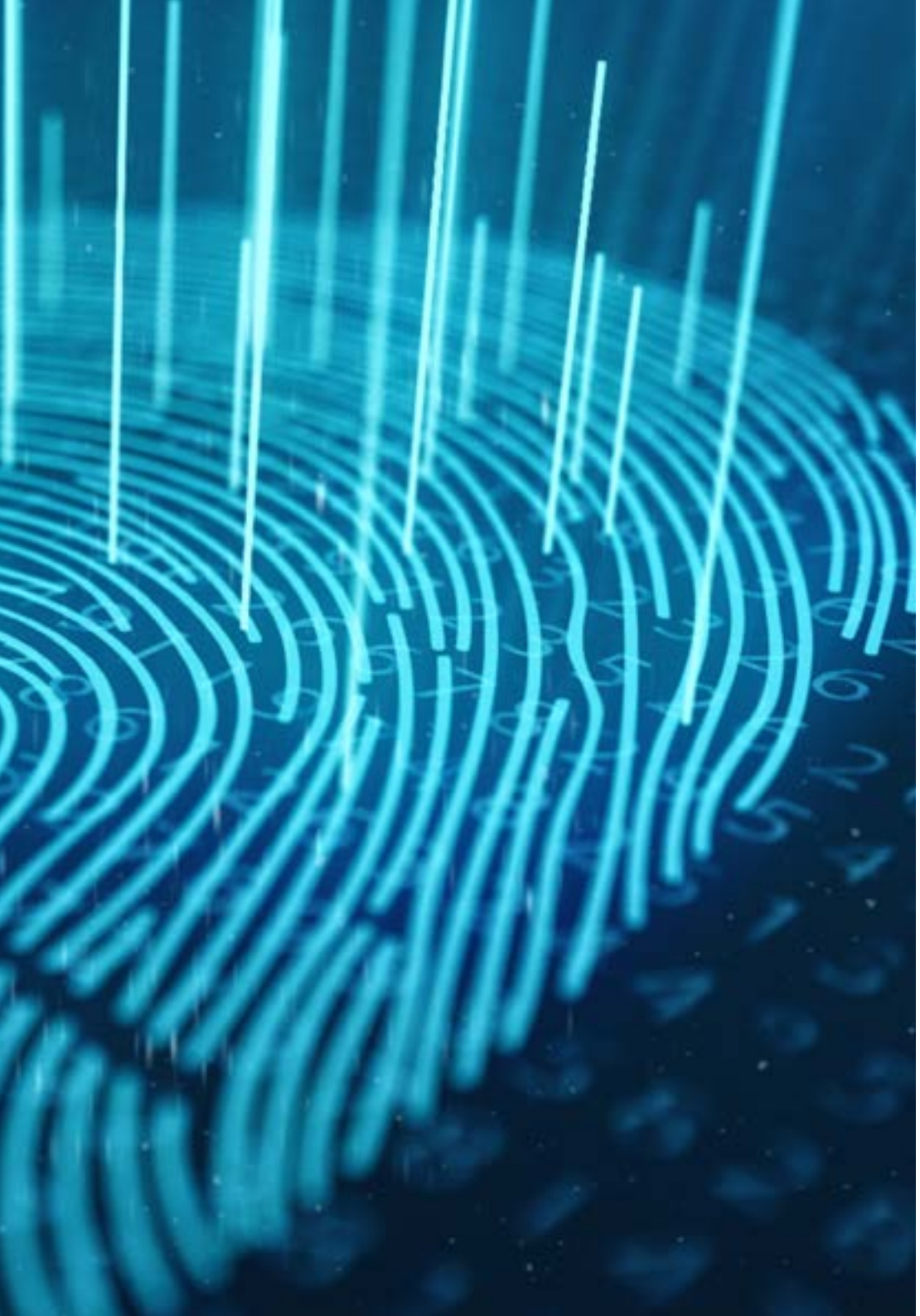
3.3. Projetos de continuidade. Tipologia
- 3.3.1. Plano de Continuidade de Negócio (PCN)
- 3.3.2. Plano de continuidade de TIC (PCTIC)
- 3.3.3. Plano de recuperação em caso de desastres (PRD)

3.4. Gestão de riscos associada ao PCN
- 3.4.1. Análise de impacto no negócio
- 3.4.2. Benefícios da implementação de um PCN
- 3.4.3. Mentalidade baseada em riscos

3.5. Ciclo de vida de um plano de continuidade de negócio
- 3.5.1. Fase 1: análise da organização
- 3.5.2. Fase 2: determinação da estratégia de continuidade
- 3.5.3. Fase 3: resposta à contingência
- 3.5.4. Fase 4: prova, manutenção e revisão

3.6. Fase de análise da organização de um PCN
- 3.6.1. Identificação de processos no âmbito do PCN
- 3.6.2. Identificação de áreas críticas do negócio
- 3.6.3. Identificação de dependências entre áreas e processos
- 3.6.4. Determinação do MTD adequado
- 3.6.5. Documentos a entregar Criação de um plano





3.7. Fase de determinação da estratégia de continuidade num PCN
  3.7.1. Funções na fase de determinação da estratégia
  3.7.2. Tarefas da fase de determinação da estratégia
  3.7.3. Documentos a entregar
3.8. Fase de resposta à contingência num PCN
  3.8.1. Funções na fase de resposta
  3.8.2. Tarefas nesta fase
  3.8.3. Documentos a entregar
3.9. Fase de testes, manutenção e revisão de um PCN
  3.9.1. Funções na fase de testes, manutenção e revisão
  3.9.2. Tarefas na fase de testes, manutenção e revisão
  3.9.3. Documentos a entregar
3.10. Normas ISO associadas aos Planos de Continuidade de Negócio (PCN)
  3.10.1. ISO 22301:2019
  3.10.2. ISO 22313:2020
  3.10.3. Outras normas ISO e internacionais relacionadas

Este Curso de Especialização permitirá aprofundar questões como a identificação de dependências entre áreas e processos, um aspeto fundamental para estabelecer uma cibersegurança correta"

05

Metodologia

Este programa de capacitação oferece uma forma diferente de aprendizagem. A nossa metodologia é desenvolvida através de um modo de aprendizagem cíclico: ***o Relearning***. Este sistema de ensino é utilizado, por exemplo, nas escolas médicas mais prestigiadas do mundo e tem sido considerado um dos mais eficazes pelas principais publicações, tais como a ***New England Journal of Medicine.***

Descubra o Relearning, um sistema que abandona a aprendizagem linear convencional para o levar através de sistemas de ensino cíclicos: uma forma de aprendizagem que provou ser extremamente eficaz, especialmente em disciplinas que requerem memorização"

Estudo de Caso para contextualizar todo o conteúdo

O nosso programa oferece um método revolucionário de desenvolvimento de competências e conhecimentos. O nosso objetivo é reforçar as competências num contexto de mudança, competitivo e altamente exigente.

Com a TECH pode experimentar uma forma de aprendizagem que abala as fundações das universidades tradicionais de todo o mundo"

Terá acesso a um sistema de aprendizagem baseado na repetição, com ensino natural e progressivo ao longo de todo o programa de estudos.

O estudante aprenderá, através de atividades de colaboração e casos reais, a resolução de situações complexas em ambientes empresariais reais.

Um método de aprendizagem inovador e diferente

Este programa da TECH é um programa de ensino intensivo, criado de raiz, que propõe os desafios e decisões mais exigentes neste campo, tanto a nível nacional como internacional. Graças a esta metodologia, o crescimento pessoal e profissional é impulsionado, dando um passo decisivo para o sucesso. O método do caso, a técnica que constitui a base deste conteúdo, assegura que a realidade económica, social e profissional mais atual é seguida.

> *O nosso programa prepara-o para enfrentar novos desafios em ambientes incertos e alcançar o sucesso na sua carreira"*

O método do caso tem sido o sistema de aprendizagem mais amplamente utilizado nas principais escolas de informática do mundo desde que existem. Desenvolvido em 1912 para que os estudantes de direito não só aprendessem o direito com base no conteúdo teórico, o método do caso consistia em apresentar-lhes situações verdadeiramente complexas, a fim de tomarem decisões informadas e valorizarem juízos sobre a forma de as resolver. Em 1924 foi estabelecido como um método de ensino padrão em Harvard.

Numa dada situação, o que deve fazer um profissional? Esta é a questão que enfrentamos no método do caso, um método de aprendizagem orientado para a ação. Ao longo do programa, os estudantes serão confrontados com múltiplos casos da vida real. Terão de integrar todo o seu conhecimento, investigar, argumentar e defender as suas ideias e decisões.

Relearning Methodology

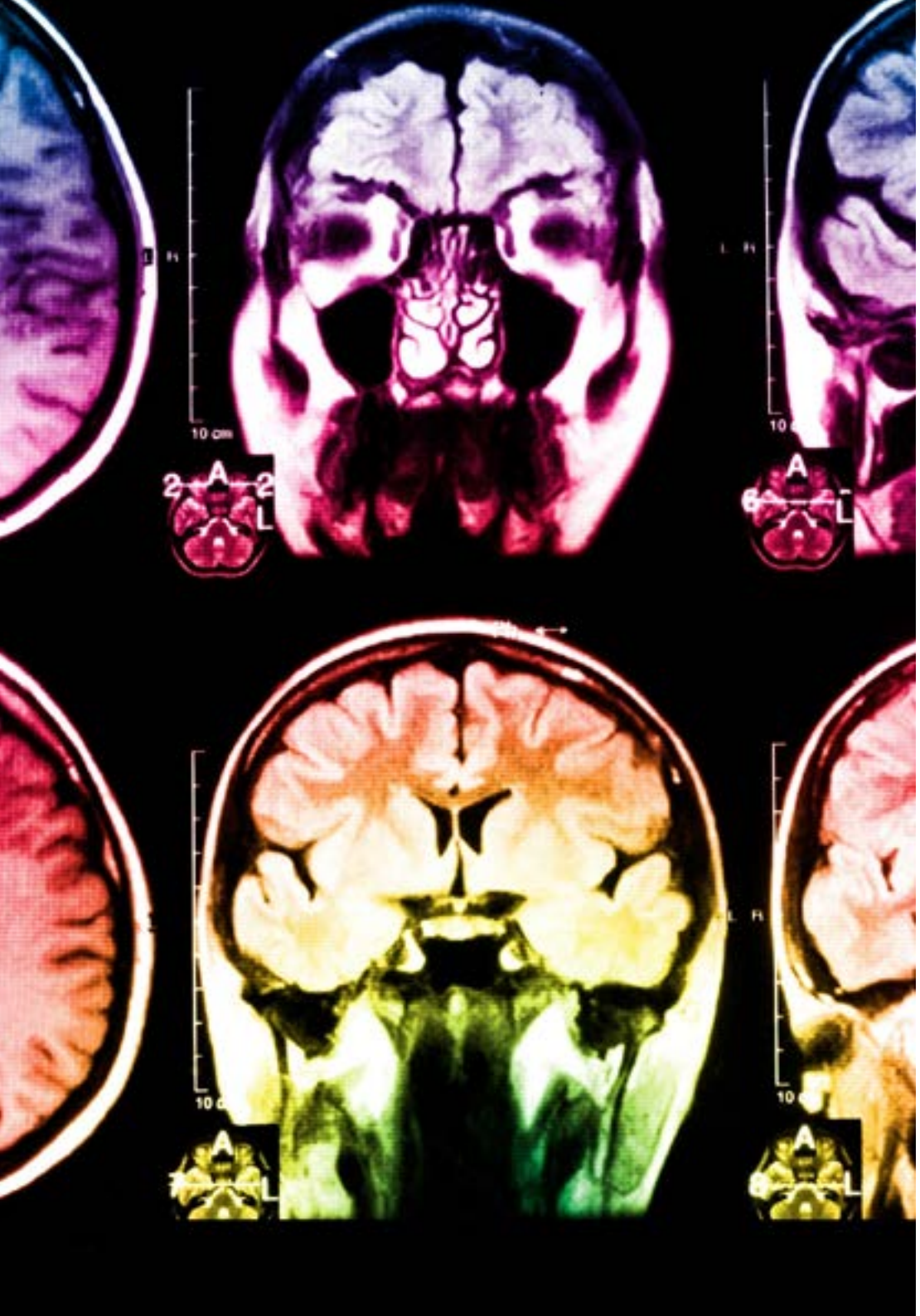
A TECH combina eficazmente a metodologia do Estudo de Caso com um sistema de aprendizagem 100% online baseado na repetição, que combina elementos didáticos diferentes em cada lição.

Melhoramos o Estudo de Caso com o melhor método de ensino 100% online: o Relearning.

Em 2019 obtivemos os melhores resultados de aprendizagem de todas as universidades online do mundo.

Na TECH aprende- com uma metodologia de vanguarda concebida para formar os gestores do futuro. Este método, na vanguarda da pedagogia mundial, chama-se Relearning.

A nossa universidade é a única universidade de língua espanhola licenciada para utilizar este método de sucesso. Em 2019, conseguimos melhorar os níveis globais de satisfação dos nossos estudantes (qualidade de ensino, qualidade dos materiais, estrutura dos cursos, objetivos...) no que diz respeito aos indicadores da melhor universidade online do mundo.



No nosso programa, a aprendizagem não é um processo linear, mas acontece numa espiral (aprender, desaprender, esquecer e reaprender). Portanto, cada um destes elementos é combinado de forma concêntrica. Esta metodologia formou mais de 650.000 licenciados com sucesso sem precedentes em áreas tão diversas como a bioquímica, genética, cirurgia, direito internacional, capacidades de gestão, ciência do desporto, filosofia, direito, engenharia, jornalismo, história, mercados e instrumentos financeiros. Tudo isto num ambiente altamente exigente, com um corpo estudantil universitário com um elevado perfil socioeconómico e uma idade média de 43,5 anos.

O Relearning permitir-lhe-á aprender com menos esforço e mais desempenho, envolvendo-o mais na sua capacitação, desenvolvendo um espírito crítico, defendendo argumentos e opiniões contrastantes: uma equação direta ao sucesso.

A partir das últimas provas científicas no campo da neurociência, não só sabemos como organizar informação, ideias, imagens e memórias, mas sabemos que o lugar e o contexto em que aprendemos algo é fundamental para a nossa capacidade de o recordar e armazenar no hipocampo, para o reter na nossa memória a longo prazo.

Desta forma, e no que se chama Neurocognitive context-dependent e-learning, os diferentes elementos do nosso programa estão ligados ao contexto em que o participante desenvolve a sua prática profissional.

Este programa oferece o melhor material educativo, cuidadosamente preparado para profissionais:

Material de estudo

Todos os conteúdos didáticos são criados pelos especialistas que irão ensinar o curso, especificamente para o curso, para que o desenvolvimento didático seja realmente específico e concreto.

Estes conteúdos são depois aplicados ao formato audiovisual, para criar o método de trabalho online da TECH. Tudo isto, com as mais recentes técnicas que oferecem peças de alta-qualidade em cada um dos materiais que são colocados à disposição do aluno.

Masterclasses

Existem provas científicas sobre a utilidade da observação por terceiros especializada.

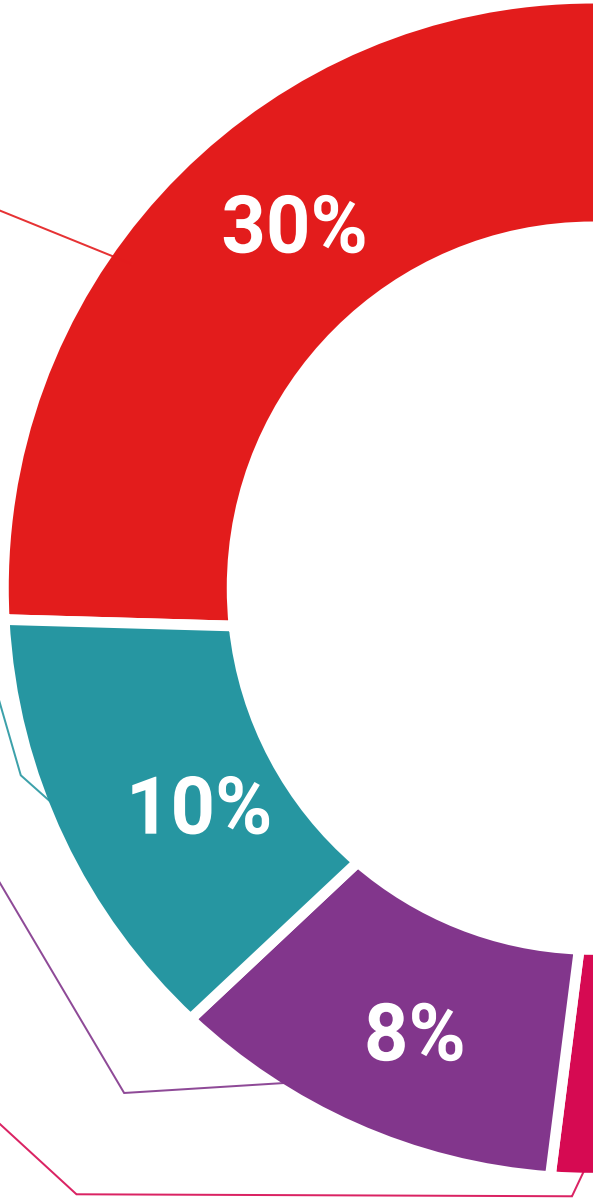
O denominado Learning from an Expert constrói conhecimento e memória, e gera confiança em futuras decisões difíceis.

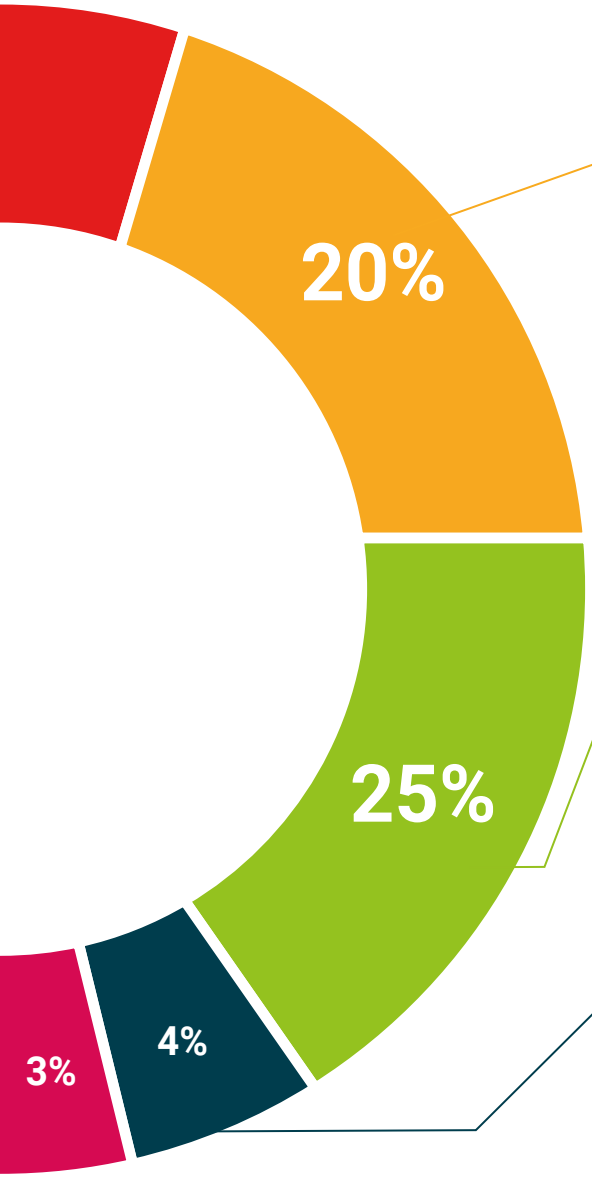
Práticas de aptidões e competências

Realizarão atividades para desenvolver competências e aptidões específicas em cada área temática. Práticas e dinâmicas para adquirir e desenvolver as competências e capacidades que um especialista necessita de desenvolver no quadro da globalização em que vivemos.

Leituras complementares

Artigos recentes, documentos de consenso e diretrizes internacionais, entre outros. Na biblioteca virtual da TECH o aluno terá acesso a tudo o que necessita para completar a sua capacitação.





Case studies

Completarão uma seleção dos melhores estudos de casos escolhidos especificamente para esta situação. Casos apresentados, analisados e instruídos pelos melhores especialistas na cena internacional.

Resumos interativos

A equipa da TECH apresenta os conteúdos de uma forma atrativa e dinâmica em comprimidos multimédia que incluem áudios, vídeos, imagens, diagramas e mapas concetuais a fim de reforçar o conhecimento.

Este sistema educativo único para a apresentação de conteúdos multimédia foi premiado pela Microsoft como uma "História de Sucesso Europeu".

Testing & Retesting

Os conhecimentos do aluno são periodicamente avaliados e reavaliados ao longo de todo o programa, através de atividades e exercícios de avaliação e auto-avaliação, para que o aluno possa verificar como está a atingir os seus objetivos.

06

Certificação

O Curso de Especialização em Administração da Segurança das Tecnologias da Informação garante, para além do conteúdo mais rigoroso e atualizado, o acesso a um certificado de Curso de Especialização emitido pela TECH Universidade Tecnológica.

Conclua este plano de estudos com sucesso e receba o seu certificado sem sair de casa e sem burocracias"

Este **Curso de Especialização em Administração da Segurança das Tecnologias da Informação** conta com o conteúdo científico mais completo e atualizado do mercado.

Uma vez aprovadas as avaliações, o aluno receberá por correio, com aviso de receção, o certificado* correspondente ao título de **Estudio** emitido pela **TECH Universidade Tecnológica.**

Este certificado contribui significativamente para o desenvolvimento da capacitação continuada dos profissionais e proporciona um importante valor para a sua capacitação universitária, sendo 100% válido e atendendo aos requisitos normalmente exigidos pelas bolsas de emprego, concursos públicos e avaliação de carreiras profissionais.

Certificação:**Curso de Especialização em Administração da Segurança das Tecnologias da Informação**

Modalidade: **online**

Duração: **6 meses**

ECTS: **18 ECTS**


tech universidade tecnológica

Concede o presente

CERTIFICADO

a

Sr./Sra. _____, com o documento de identificação nº_____

Por ter completado e certificado com sucesso o

CURSO DE ESPECIALIZAÇÃO

em

Administração da Segurança das Tecnologias da Informação

Este é um certificado atribuído por esta Universidade, reconhecido por 18 ECTS e equivalente a 450 horas, com data de início a dd/mm/aaaaa e data de conclusão a dd/mm/aaaaa.

A TECH é uma Instituição Privada de Ensino Superior reconhecida pelo Ministério da Educação Pública a partir de 28 de junho de 2018.

A 17 de junho de 2020

código único TECH: AFWOR23S techtitute.com/titulos

*Apostila de Haia: Caso o aluno solicite que o seu certificado seja apostilado, a TECH EDUCATION providenciará a obtenção do mesmo a um custo adicional.

tech universidade tecnológica

Curso de Especialização

Administração da Segurança das Tecnologias da Informação

- Modalidade: **Online**
- Duração: **6 meses**
- Certificação: **TECH Universidade Tecnológica**
- Créditos: **18 ECTS**
- Horário: **Ao seu próprio ritmo**
- Exames: **Online**

Curso de Especialização

Administração da Segurança das Tecnologias da Informação

tech universidade tecnológica