उच्च स्नातकोत्तर उपाधि

सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधि

tech global university

tech global university

उच्च स्नातकोत्तर उपाधि

सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधि

- रुपात्मकता: ऑनलाइन
- अवधि: 2 वर्ष
- उपाधि: TECH Global University
- प्रमाणन: 120 ECTS
- अनुसूची: अपनी गति से
- परीक्षा: ऑनलाइन

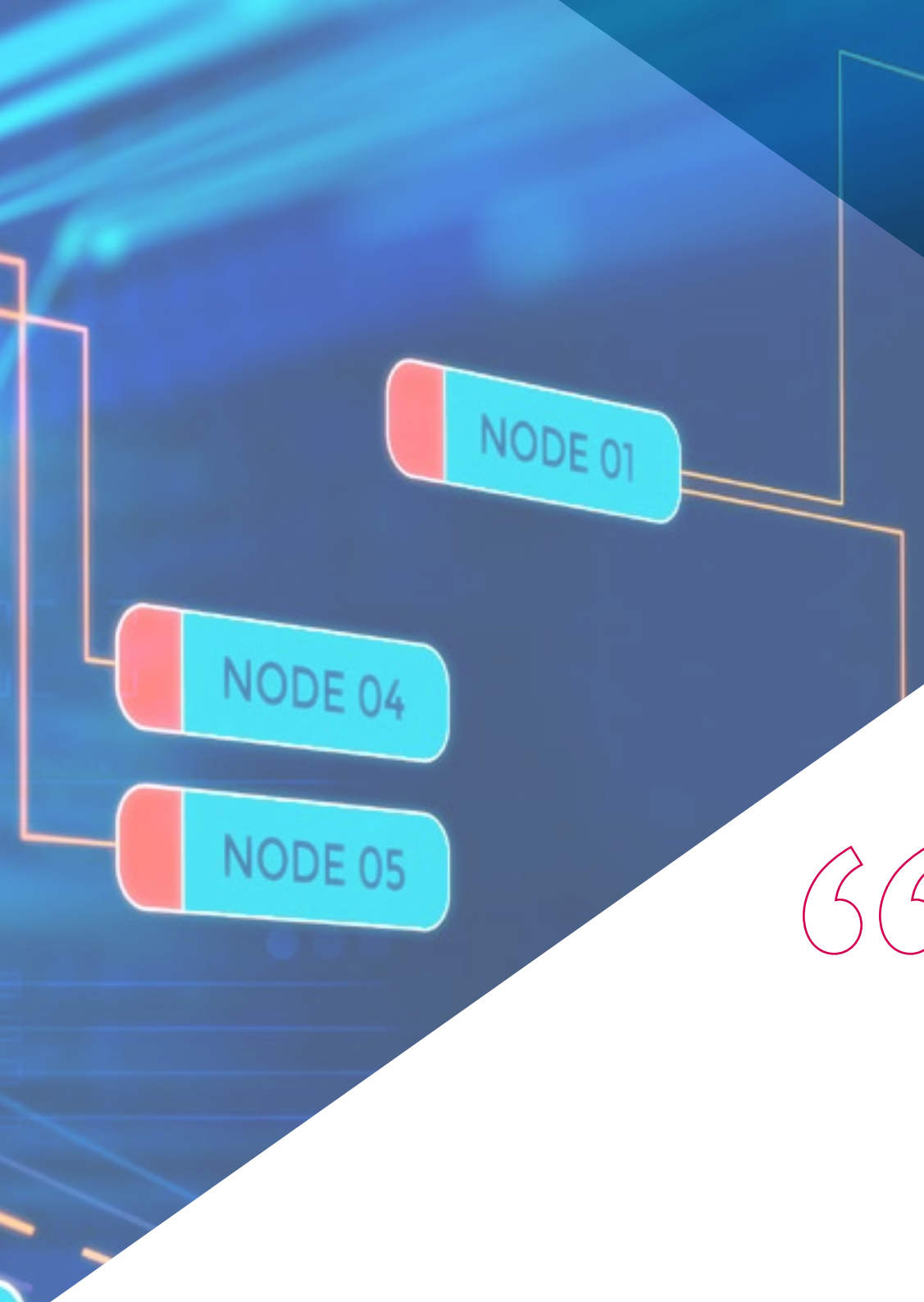
वेब पेज: www.techtitute.com/in/information-technology/advanced-master-degree/advanced-master-degree-secure-information-management

सूची

01

प्रस्तुतिकरण

आज की दुनिया पर डिजिटल वातावरण का बोलबाला है। यह विभिन्न क्षेत्रों में बड़ी संख्या में गतिविधियों का प्रबंधन करता है। इसलिए, इंटरनेट और सभी मौजूदा ऑनलाइन टूल के बिना अवकाश, काम या दोस्तों के साथ संपर्क और परिवार के साथ अवकाश, काम या दोस्तों और परिवार के साथ संपर्क की कल्पना करना कठिन है। इस कारण से, सोशल नेटवर्क और मैसेजिंग एप्लिकेशन के माध्यम से बातचीत में अहानिकर डेटा से लेकर बैंकिंग या व्यावसायिक वेबसाइटों पर होस्ट की गई अत्यधिक संवेदनशील व्यक्तिगत और व्यावसायिक जानकारी तक, बड़ी मात्रा में जानकारी दैनिक आधार पर स्थानांतरित की जाती है। इस जटिल परिदृश्य में, कंपनियों को ऐसे विशेषज्ञों की आवश्यकता होती है जो अपनी सुरक्षा पर पर्याप्त ध्यान देते हुए इन क्षेत्रों से संबंधित सभी प्रकार की जानकारी का प्रबंधन कर सकें। कई कंपनियाँ अपनी जानकारी सुरक्षित रखने के लिए इस प्रोफ़ाइल वाले कर्मियों की तलाश कर रही हैं।



“हर दिन दुर्भावनापूर्ण लोग उन कंपनियों और संस्थानों की सुरक्षा से समझौता करने की कोशिश करते हैं जो बहुत मूल्यवान डेटा का प्रबंधन करते हैं: आप उस जानकारी के महान रक्षक हो सकते हैं”

हर दिन लाखों लोग इंटरनेट पर हर तरह की गतिविधियाँ करते हैं। वे समाचार देखते हैं, दोस्तों और परिवार के साथ चैट करते हैं, सोशल नेटवर्क पर राय साझा करते हैं, विभिन्न कंपनियों और संस्थानों में प्रशासनिक कार्य करते हैं, सभी प्रकार की फाइलें साझा करते हैं या काम से संबंधित कार्य करते हैं। इसलिए, दुनिया भर में हर पल अनगिनत मात्रा में डेटा बनाया और स्थानांतरित किया जा रहा है।

उन्हें पर्याप्त सुरक्षा के साथ प्रबंधित करना कोई आसान काम नहीं है, क्योंकि इसके लिए विभिन्न क्षेत्रों से विशिष्ट ज्ञान की आवश्यकता होती है जो आम तौर पर एक-दूसरे के संपर्क में नहीं होंगे। इस कारण से, सुरक्षित सूचना प्रबंधन में यह उच्च स्नातकोत्तर उपाधि उन सभी इंजीनियरों और आईटी पेशेवरों के लिए एक उत्कृष्ट अवसर है जो दोनों क्षेत्रों में शीर्ष विशेषज्ञ बनने के लिए सूचना प्रबंधन और साइबर सुरक्षा को एकीकृत करना चाहते हैं।

कई कंपनियाँ और संस्थान अत्यधिक संवेदनशील और मूल्यवान डेटा को संभालते हैं जिसके लिए उचित प्रशासन, संरक्षण और निगरानी की आवश्यकता होती है। दोनों विषयों में अभी भी बहुत से विशेषज्ञ नहीं हैं जो कार्यभार संभाल सकें और सभी पहलुओं का पर्याप्त रूप से प्रबंधन कर सकें। इसलिए, जो छात्र इस उच्च स्नातकोत्तर उपाधि को पूरा करते हैं, वे उन कंपनियों में शीर्ष पदों तक पहुंचने के लिए पूरी तरह से तैयार होंगे जो अपनी डिजिटल जानकारी सुरक्षित करना चाहते हैं।

इस उद्देश्य से, TECH ने सर्वोत्तम सामग्री डिज़ाइन की है और इन क्षेत्रों में व्यापक पेशेवर अनुभव वाले सर्वश्रेष्ठ शिक्षकों को एक साथ लाया है, ताकि छात्रों को यथासंभव संपूर्ण शिक्षा प्राप्त हो और वे कार्यस्थल में प्रगति कर सकें।

यह **सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधि में उच्च स्नातकोत्तर उपाधि** बाजार का सबसे पूर्ण और अद्यतन कार्यक्रम प्रदान करता है। इसकी सबसे उल्लेखनीय विशेषताएं हैं:

- कंप्यूटर विज्ञान विशेषज्ञों द्वारा प्रस्तुत केस स्टडीज का विकास
- ग्राफिक, योजनाबद्ध, और प्रमुख रूप से व्यावहारिक विषयवस्तु जिसके साथ वे बनाए गए हैं, पेशेवर अभ्यास के लिए आवश्यक विषयों पर वैज्ञानिक और व्यावहारिक जानकारी प्रदान करते हैं
- व्यावहारिक अभ्यास जहां सीखने में सुधार के लिए स्व-मूल्यांकन का उपयोग किया जा सकता है
- डिजिटल डेटा समन्वयन विभाग और सुरक्षा में नवीन पद्धतियों पर इसका विशेष जोर है
- सैद्धांतिक पाठ, विशेषज्ञ से प्रश्न, विवादास्पद विषयों पर वाद-विवाद मंच, और व्यक्तिगत चिंतन असाइनमेंट
- वह सामग्री जो इंटरनेट कनेक्शन के साथ किसी भी स्थिर या पोर्टेबल उपकरणों से पहुंच योग्य है

> डिजिटल क्षेत्र में हम जो कुछ भी करते हैं वह रिकॉर्ड किया जाता है। इस उच्च स्नातकोत्तर उपाधि की बदौलत इंटरनेट को एक सुरक्षित स्थान बनाएँ"

जब आप इस कार्यक्रम को पूरा करेंगे तो देश की सर्वश्रेष्ठ कंपनियाँ अपने डेटा के प्रबंधन और सुरक्षा को लेकर आप पर भरोसा करेंगी"

यह उच्च स्नातकोत्तर उपाधि आपके करियर के भविष्य के लिए दो आवश्यक विषयों को जोड़ती है। अभी नामांकन करें और अपने सभी लक्ष्य प्राप्त करें।

डेटा प्रबंधन और डेटा सुरक्षा के बारे में सब कुछ जानें और देखें कि आप बहुत कम समय में पेशेवर रूप से कैसे आगे बढ़ते हैं।

इसके शिक्षण स्टाफ में प्रतिष्ठित संदर्भ समाजों और विश्वविद्यालयों के मान्यता प्राप्त विशेषज्ञों के अलावा, क्षेत्र से संबंधित पेशेवर शामिल हैं, जो इस कार्यक्रम में अपने काम का अनुभव लाते हैं।

नवीनतम शैक्षिक प्रौद्योगिकी के साथ विकसित मल्टीमीडिया सामग्री, पेशेवर को स्थित और प्रासंगिक शिक्षा प्रदान करेगी, यानी, एक अनुरूपित वातावरण जो वास्तविक जीवन स्थितियों के लिए प्रशिक्षित करने के लिए डिज़ाइन किया गया एक गहन सीखने का अनुभव प्रदान करेगा।

यह कार्यक्रम समस्या-आधारित शिक्षा के आसपास तैयार किया गया है, जिससे पेशेवर को शैक्षणिक वर्ष के दौरान उत्पन्न होने वाली विभिन्न व्यावसायिक अभ्यास स्थितियों को हल करने का प्रयास छात्र चाहिए। इस उद्देश्य के लिए, पेशेवर को प्रसिद्ध और अनुभवी विशेषज्ञों द्वारा बनाई गई एक अभिनव सहभागी वीडियो प्रणाली द्वारा सहायता प्रदान की जाएगी।

02

उद्देश्य

सुरक्षित सूचना प्रबंधन में इस उच्च स्नातकोत्तर उपाधि का मुख्य उद्देश्य छात्रों को कंप्यूटर विज्ञान और इंजीनियरिंग की दो अलग लेकिन परस्पर संबंधित शाखाओं में सर्वोत्तम ज्ञान प्रदान करना है: डिजिटल वातावरण में डेटा प्रबंधन और साइबर सुरक्षा। इन दोनों क्षेत्रों को मिलाकर, इस कार्यक्रम को लेने वाले कंप्यूटर वैज्ञानिक और पेशेवर अपने करियर में आने वाली हर स्थिति में सर्वोत्तम समाधान लागू करने में सक्षम होंगे, सभी प्रकार की संवेदनशील जानकारी को प्रबंधित और संरक्षित करने के लिए अपनी कंपनियों को सबसे उपयुक्त उपकरण प्रदान करेंगे।

आपका लक्ष्य आपकी कंपनी में सर्वश्रेष्ठ विशेषज्ञ बनना है और TECH आपको इसे प्राप्त करने के लिए उपकरण प्रदान करता है”

सामान्य उद्देश्य

- कंपनी के प्रत्येक विभाग में डेटा विश्लेषिकी तकनीकों को के अनुप्रयोग को करने के लाभों का विश्लेषण करें
- प्रत्येक विभाग की जरूरतों और अनुप्रयोगों को समझने के लिए आधार विकसित करें
- सही उपकरण का चयन करने के लिए विशेष ज्ञान उत्पन्न करें
- विभाग के अनुसार जितना संभव हो उतना उत्पादक होने के लिए तकनीकों और उद्देश्यों का प्रस्ताव करें
- साइबर विश्लेषकों के की भूमिका का विश्लेषण करें
- सोशल इंजीनियरिंग और इसकी विधियों के बारे में गहराई से जानें
- OSINT, HUMINT, OWASP, PTEC, OSSTM और OWISAM पद्धतियों की जांच करें
- जोखिम विश्लेषण करें और जोखिम मेट्रिक्स को समझें
- गुमनामी का उचित उपयोग और टीओआर, I2P और फ्रीनेट जैसे नेटवर्क का उपयोग निर्धारित करें
- वर्तमान साइबर सुरक्षा नियमों को संकलित करें
- सुरक्षा ऑडिट करने के लिए विशेष ज्ञान उत्पन्न करें
- उचित उपयोग नीतियां विकसित करें
- सबसे महत्वपूर्ण खतरे का पता लगाने और रोकथाम प्रणालियों की जांच करें
- नए खतरे का पता लगाने वाली प्रणालियों का मूल्यांकन करें, साथ ही अधिक पारंपरिक समाधानों के संबंध में उनके विकास का भी मूल्यांकन करें
- मुख्य वर्तमान मोबाइल प्लेटफ़ॉर्म, उनकी विशेषताओं और उपयोग का विश्लेषण करें
- IoT परियोजना भागों के सुरक्षा जोखिमों को पहचानें, विश्लेषण करें और उनका आकलन करें
- प्राप्त जानकारी का मूल्यांकन करें और रोकथाम और हैकिंग तंत्र विकसित करें
- साइबर सुरक्षा परिवेश में रिवर्स इंजीनियरिंग लागू करें
- विकसित सॉफ़्टवेयर पर किए जाने वाले परीक्षणों को निर्दिष्ट करें
- फोरेंसिक रिपोर्ट बनाने के लिए सभी मौजूदा साक्ष्य और डेटा एकत्र करें
- फोरेंसिक रिपोर्ट विधिवत प्रस्तुत करें
- कंप्यूटर सुरक्षा की वर्तमान और भविष्य की स्थिति का विश्लेषण करें
- नई उभरती प्रौद्योगिकियों के जोखिमों की जांच करें
- कंप्यूटर सुरक्षा के संबंध में विभिन्न तकनीकों का संकलन करें

> साइबर सुरक्षा और डेटा प्रबंधन तेजी से आगे बढ़ने वाले विषय हैं। यह उच्च स्नातकोत्तर उपाधि लें और नवीनतम ज्ञान प्राप्त करें"

विशिष्ट उद्देश्य

मॉड्यूल 1. एक व्यावसायिक संस्था में डेटा विश्लेषिकी

- गुणवत्तापूर्ण निर्णय लेने के लिए विश्लेषणात्मक कौशल विकसित करें
- प्रभावी विपणन और संचार अभियानों की जांच करें
- विभाग के अनुसार स्कोरकार्ड और केपीआई के निर्माण का निर्धारण करें
- भविष्य कहनेवाला विश्लेषण विकसित करने के लिए विशेष ज्ञान उत्पन्न करें
- बाजार अनुसंधान के आधार पर व्यवसाय और वफादारी योजनाओं का प्रस्ताव
- ग्राहक को सुनने की क्षमता विकसित करें
- वास्तविक स्थितियों में सांख्यिकीय, मात्रात्मक और तकनीकी ज्ञान लागू करें

मॉड्यूल 2. डेटा प्रबंधन, डेटा हेरफेर और डेटा साइंस रिपोर्टिंग

- डेटा विश्लेषण करें
- विविध डेटा को एकीकृत करें: सूचना की स्थिरता प्राप्त करना
- निर्णय लेने के लिए प्रासंगिक, प्रभावी जानकारी तैयार करना
- इसकी टाइपोलॉजी और उपयोग के अनुसार डेटा प्रबंधन के लिए सर्वोत्तम प्रथाओं का निर्धारण करें
- डेटा पहुँच और पुन: उपयोग नीतियाँ स्थापित करें
- सूचना की सुरक्षा और उपलब्ध: उपलब्धता, अखंडता और गोपनीयता सुनिश्चित करना
- प्रोग्रामिंग भाषाओं का उपयोग करके डेटा प्रबंधन के लिए उपकरणों की जांच करें

मॉड्यूल 3. डेटा साइंस की नींव के रूप में IoT उपकरणों और प्लेटफ़ॉर्म

- पहचानें कि IoT (इंटरनेट ऑफ़ थिंग्स) और IIoT (इंडस्ट्रियल इंटरनेट ऑफ़ थिंग्स) क्या है
- इन्डस्ट्रीअल इंटरनेट कंसोर्टियम की जांच करें
- विश्लेषण करें कि आईओटी संदर्भ वास्तुकला क्या है
- आईओटी सेंसर और उपकरणों और उनके वर्गीकरण का संबोधन
- आईओटी में उपयोग किए जाने वाले संचार प्रोटोकॉल और प्रौद्योगिकियों की पहचान करें
- IoT में विभिन्न क्लाउड प्लेटफ़ॉर्म की जाँच करें: सामान्य प्रयोजन, औद्योगिक और खुला स्रोत
- डेटा विनिमय तंत्र विकसित करें
- सुरक्षा आवश्यकताओं और रणनीतियों को स्थापित करें
- विभिन्न आईओटी और आईआईओटी अनुप्रयोग क्षेत्रों को प्रस्तुत करें

मॉड्यूल4.डेटा विश्लेषण के लिए ग्राफिकल प्रतिनिधित्व

- डेटा प्रतिनिधित्व और विश्लेषण में विशेष ज्ञान उत्पन्न करें
- विभिन्न प्रकार के समूहीकृत डेटा की जाँच करें
- विभिन्न क्षेत्रों में सबसे अधिक उपयोग किए जाने वाले ग्राफिकल अभ्यावेदन स्थापित करें
- डेटा दृश्यावलोकन में डिजाइन के निर्धारित करें
- ग्राफिक कथा को एक उपकरण के रूप में प्रस्तुत करें
- ग्राफ़िंग और खोजपूर्ण डेटा विश्लेषण के लिए विभिन्न सॉफ़्टवेयर उपकरणों का विश्लेषण करें

मॉड्यूल 5. साइंस डेटा उपकरण

- डेटा को जानकारी में बदलने के कौशल विकसित करें जिससे ज्ञान संचित किया जा सकता है
- किसी डेटासेट की मुख्य विशेषताओं, इसकी संरचना, घटकों और मॉडलिंग में इसके वितरण के निहितार्थ का निर्धारण करें
- अग्रिम में व्यापक डेटा विश्लेषण करके निर्णय लेने का समर्थन करें
- डेटा विज्ञान तकनीकों का उपयोग करके व्यावहारिक मामलों को हल करने के लिए कौशल विकसित करें
- निष्पादित प्रीप्रोसेसिंग के आधार पर प्रत्येक डेटासेट को मॉडलिंग करने के लिए सबसे उपयुक्त सामान्य उपकरण और तरीके स्थापित करें
- विभिन्न मेट्रिक्स पर चुनी गई रणनीति के प्रभाव को समझते हुए, विश्लेषणात्मक रूप से परिणामों का मूल्यांकन करें
- पूर्वप्रसंस्करण या मॉडलिंग विधियों को लागू करने के बाद प्राप्त परिणामों के महत्वपूर्ण की क्षमता प्रदर्शन करें

मॉड्यूल 6. डेटा माइनिंग चयन, प्रसंस्करण और परिवर्तन

- किसी भी डेटा विश्लेषण और मूल्यांकन के लिए सांख्यिकीय पूर्वापेक्षाओं के बारे में विशेष ज्ञान उत्पन्न करें
- डेटा पहचान, तैयारी और परिवर्तन के लिए आवश्यक कौशल विकसित करें
- प्रस्तुत विभिन्न पद्धतियों का मूल्यांकन करें और फायदे और नुकसान की पहचान करें
- डेटा प्रीप्रोसेसिंग के लिए उपयोग किए जाने वाले एल्गोरिदम के कार्यान्वयन का विकास करें
- डेटा प्री-प्रोसेसिंग के लिए उपयोग किए जाने वाले एल्गोरिदम के कार्यान्वयन को विकसित करता है"
- वर्णनात्मक विश्लेषण के लिए डेटा दृश्यावलोकन की व्याख्या करने की क्षमता प्रदर्शित करें
- डेटा सफाई, सामान्यीकरण और परिवर्तन के लिए विभिन्न मौजूदा डेटा तैयारी तकनीकों पर उन्नत ज्ञान विकसित करें

मॉड्यूल 7. संभाव्यता सिद्धांत का पूर्वानुमान और विश्लेषण

- समय श्रृंखला का विश्लेषण करें
- अनौपचारिक समय श्रृंखला मॉडल के सूत्रीकरण और बुनियादी गुणों का विकास करें
- मॉडलिंग की प्रणाली और वास्तविक समय श्रृंखला की भविष्यवाणी की जांच करें
- आउटलेर्स सहित अविभाज्य मॉडल निर्धारित करें
- गतिशील प्रतिगमन मॉडल लागू करें और देखी गई श्रृंखला से ऐसे मॉडल के निर्माण के लिए प्रणाली लागू करें
- अविभाज्य समय श्रृंखला के वर्णक्रमीय विश्लेषण के साथ-साथ आवधिक-आधारित अनुमान और इसकी व्याख्या से संबंधित मूलभूत पहलुओं को संबोधित करें
- किसी दिए गए समय क्षितिज के लिए समय श्रृंखला की संभावना और प्रवृत्ति का अनुमान लगाएँ

मॉड्यूल 8. इंटेलिजेंट प्रणाली का डिजाइन और विकास

- सूचना से ज्ञान की ओर संक्रमण का विश्लेषण करें
- विभिन्न प्रकार की मशीन लर्निंग तकनीकों का विकास करें
- मॉडल की गुणवत्ता निर्धारित करने के लिए मैट्रिक्स और स्कोर की जांच करें
- विभिन्न मशीन लर्निंग एल्गोरिदम लागू करें
- संभाव्य तर्क मॉडल की पहचान करें
- गहरी शिक्षा के लिए नींव रखें
- विभिन्न मशीन लर्निंग एल्गोरिदम को समझने के लिए अर्जित कौशल का प्रदर्शन करें

मॉड्यूल 9. डेटा-सघन प्रणाली और वास्तुकला

- बड़े पैमाने पर डेटा उपयोग प्रणालियों की आवश्यकताओं को निर्धारित करना
- विभिन्न डेटा मॉडल की जाँच करें और डेटाबेस का विश्लेषण करें
- वितरित प्रणालियों के लिए प्रमुख कार्यात्मकताओं और विभिन्न प्रकार की प्रणालियों में उनके महत्व का विश्लेषण करें
- मूल्यांकन करें कि कौन से व्यापक रूप से उपयोग किए जाने वाले अनुप्रयोग अपने प्रणाली को डिजाइन करने के लिए वितरित प्रणालियों के मूल सिद्धांतों का उपयोग करते हैं
- डेटाबेस द्वारा जानकारी संग्रहीत करने और पुनर्प्राप्त करने के तरीके का विश्लेषण करें
- विभिन्न प्रतिकृति मॉडल और संबंधित समस्याओं को निर्दिष्ट करें
- विभाजन और वितरित लेनदेन के तरीके विकसित करना
- बैच प्रणाली और (निकट) वास्तविक समय प्रणाली निर्धारित करें

मॉड्यूल 10. व्यापार क्षेत्रों में डेटा विज्ञान का व्यावहारिक अनुप्रयोग

- कृत्रिम बुद्धिमता (एआई) और डेटा विश्लेषिकी की कला का विश्लेषण करें
- सबसे व्यापक रूप से उपयोग की जाने वाली प्रौद्योगिकियों के विशेष ज्ञान का विकास
- उपयोग के मामलों के माध्यम से प्रौद्योगिकी की बेहतर समझ उत्पन्न करें
- लागू करने के लिए सर्वोत्तम तकनीकों का चयन करने के लिए चुनी गई रणनीतियों का विश्लेषण करें
- आवेदन के क्षेत्रों का निर्धारण करें
- लागू प्रौद्योगिकी के वास्तविक और संभावित जोखिमों की जांच करें
- उपयोग से प्राप्त लाभों का प्रस्ताव करें
- विशिष्ट सेक्टर्स में भविष्य के रुझानों की पहचान करें

मॉड्यूल 11. साइबरइंटेलिजेंस और साइबर सुरक्षा

- साइबर सुरक्षा में उपयोग की जाने वाली प्रणाली विकसित करें।
- खुफिया चक्र की जांच करें और साइबरइंटेलिजेंस में इसके अनुप्रयोग को स्थापित करें
- खुफिया विश्लेषक की भूमिका और निकासी गतिविधि में आने वाली बाधाओं का निर्धारण करें
- खुफिया उत्पादन के लिए सबसे आम उपकरण स्थापित करें
- जोखिम विश्लेषण करें और उपयोग किए गए मेट्रिक्स को समझें
- गुमनामी के विकल्पों और टीओआर, I2P, फ्रीनेट जैसे नेटवर्क के उपयोग का गहन ज्ञान प्राप्त करें
- साइबर सुरक्षा में वर्तमान नियमों का विवरण दें
- व्यक्तिगत और व्यावसायिक डेटा के लिए बैकअप नीतियाँ निर्दिष्ट करें

मॉड्यूल 12. मेज़बान सुरक्षा

- विशिष्ट सुरक्षा समस्याओं का समाधान प्रदान करने के लिए विभिन्न उपकरणों का मूल्यांकन करें
- अद्यतन प्रणाली के लिए तंत्र स्थापित करें
- घुसपैठियों के लिए उपकरण स्कैन करें
- प्रणाली एक्सेस नियम निर्धारित करें
- धोखाधड़ी से बचने के लिए मेल की जांच करें और उन्हें वर्गीकृत करें
- अनुमत सॉफ़्टवेयर की सूची तैयार करें
- सुरक्षा के लिए परिधि की पहचान करने के लिए वर्तमान नेटवर्क वास्तुकला का विश्लेषण करें

मॉड्यूल 13. नेटवर्क सुरक्षा (परिधि)

- सबसे आम हमलों को कम करने के लिए विशिष्ट फ़ायरवॉल और लिनक्स विन्यास विकसित करें
- स्नॉर्ट और सुरीकाटा जैसे सबसे अधिक उपयोग किए जाने वाले समाधानों के साथ-साथ उनके विन्यास को संकलित करें
- क्लाउड वातावरण में अगली पीढ़ी के फ़ायरवॉल और नेटवर्क कार्यात्मकताओं द्वारा प्रदान की गई विभिन्न अतिरिक्त परतों की जाँच करें
- नेटवर्क सुरक्षा के लिए उपकरण निर्धारित करें और प्रदर्शित करें कि वे बहुपरत सुरक्षा के लिए मौलिक क्यों हैं
- आसान लक्ष्य बनने से बचने के लिए विभिन्न आक्रमण वाहकों की जाँच करें

मॉड्यूल 14. स्मार्टफ़ोन सुरक्षा

- मुख्य हमलों और मैलवेयर के प्रकारों का निर्धारण करें जिनसे मोबाइल उपकरणों के उपयोगकर्ता प्रभावित होते हैं
- विन्यास में अधिक सुरक्षा स्थापित करने के लिए सबसे वर्तमान उपकरणों का विश्लेषण करें
- iOS और एंड्रॉइड दोनों प्लेटफार्मों पर प्रवेश परीक्षण करने के लिए मुख्य चरण निर्दिष्ट करें
- विभिन्न सुरक्षा और सुरक्षा उपकरणों के बारे में विशेष ज्ञान विकसित करें
- मोबाइल उपकरणों-उन्मुख प्रोग्रामिंग में सर्वोत्तम अभ्यास स्थापित करें
- मुख्य IoT वास्तुकला का विश्लेषण करें

मॉड्यूल 15. आईओटी सुरक्षा

- कनेक्टिविटी प्रौद्योगिकियों की जांच करें
- मुख्य एप्लिकेशन प्रोटोकॉल विकसित करें
- मौजूदा उपकरणों के विभिन्न प्रकार निर्दिष्ट करें
- जोखिम के स्तर और ज्ञात कमजोरियों का आकलन करें
- सुरक्षित उपयोग नीतियां विकसित करें
- इन उपकरणों के लिए उपयोग की उचित शर्तें स्थापित करें
- IOSINT तरीकों का परीक्षण करना

मॉड्यूल 16. नैतिक हैकिंग

- सार्वजनिक मीडिया में उपलब्ध जानकारी संकलित करें
- सक्रिय मोड जानकारी के लिए नेटवर्क स्कैन करें
- परीक्षण प्रयोगशालाएँ विकसित करें
- प्रदर्शन परीक्षण के लिए उपकरणों का विश्लेषण करें
- प्रणाली की विभिन्न कमजोरियों को सूचीबद्ध करें और उनका आकलन करें
- विभिन्न हैकिंग पद्धतियों को निर्दिष्ट करें

मॉड्यूल 17. रिवर्स इंजीनियरिंग

- एक कंपाइलर के चरणों का विश्लेषण करें
- x86 प्रोसेसर वास्तुकला और एआरएम प्रोसेसर वास्तुकला की जांच करें
- विश्लेषण के विभिन्न प्रकार निर्धारित करें
- विभिन्न वातावरणों में सैंडबॉक्सिंग लागू करें
- विभिन्न मैलवेयर विश्लेषण तकनीकें विकसित करें
- मैलवेयर विश्लेषण-उन्मुख उपकरण स्थापित करें

मॉड्यूल 18. सुरक्षित विकास

- सुरक्षित तरीके से किसी एप्लिकेशन के सही संचालन के लिए आवश्यक आवश्यकताओं को स्थापित करें
- त्रुटि संदेशों को समझने के लिए लॉग फ़ाइलों की जाँच करें
- विभिन्न घटनाओं का विश्लेषण करें और तय करें कि उपयोगकर्ता को क्या दिखाना है और लॉग में क्या रखना है
- एक साफ-सुथरा, आसानी से सत्यापन योग्य और गुणवत्ता वाला कोड तैयार करें
- विकास के प्रत्येक चरण के लिए उपयुक्त दस्तावेज़ीकरण का मूल्यांकन करें
- प्रणाली को अनुकूलित करने के लिए सर्वर का व्यवहार निर्दिष्ट करें
- मॉड्यूलर, पुन: प्रयोज्य और रखरखाव योग्य कोड विकसित करें

मॉड्यूल 19. फोरेंसिक विश्लेषण

- किसी अपराध का सबूत देने वाले विभिन्न तत्वों की पहचान करें
- विभिन्न मीडिया से डेटा खो जाने से पहले प्राप्त करने के लिए विशेष ज्ञान उत्पन्न करें
- जानबूझकर हटाए गए डेटा की पुनर्प्राप्ति
- प्रणाली लॉग और रिकॉर्ड का विश्लेषण करें
- निर्धारित करें कि डेटा को कैसे डुप्लिकेट किया जाए ताकि मूल में कोई बदलाव न हो
- निरंतरता के लिए साक्ष्य को प्रमाणित करें
- एक ठोस और निर्बाध रिपोर्ट तैयार करें
- निष्कर्षों को सुसंगत ढंग से प्रस्तुत करें
- सक्षम प्राधिकारी के समक्ष रिपोर्ट का बचाव कैसे करें यह स्थापित करें
- सुरक्षित दूरसंचार के लिए रणनीतियाँ निर्दिष्ट करें

मॉड्यूल 20. IT सुरक्षा में वर्तमान और भविष्य की चुनौतियाँ

- क्रिप्टोकरेंसी के उपयोग, अर्थव्यवस्था और सुरक्षा पर प्रभाव की जांच करें
- उपयोगकर्ताओं की स्थिति और डिजिटल निरक्षरता की उपाधि का विश्लेषण करें
- ब्लॉकचेन के उपयोग का दायरा निर्धारित करें
- नेटवर्क एड्रेसिंग में IPv4 के विकल्प प्रस्तुत करें
- प्रौद्योगिकियों के सही उपयोग में जनसंख्या को शिक्षित करने के लिए रणनीतियाँ विकसित करें
- नई सुरक्षा चुनौतियों का सामना करने और पहचान की चोरी को रोकने के लिए विशेष ज्ञान उत्पन्न करें
- सुरक्षित दूरसंचार के लिए रणनीतियाँ निर्दिष्ट करें

03

कौशल

सुरक्षित सूचना प्रबंधन में इस उच्च स्नातकोत्तर उपाधि को पूरा करने वाले छात्र डेटा प्रबंधन और साइबर सुरक्षा के क्षेत्र में बड़ी संख्या में अत्यधिक विशिष्ट कार्य करने में सक्षम होंगे। इसलिए, यह डिग्री पूरक ज्ञान प्रदान करने के लिए दोनों शाखाओं को जोड़ती है जिसे पार किया जा सकता है और विभिन्न स्थितियों और पेशेवर वातावरण में उपयोग किया जा सकता है। इस तरह, छात्र एक व्यापक सीखने की प्रक्रिया से गुजरेंगे जो उन्हें क्षेत्र में सच्चे विशेषज्ञ बनने के लिए मार्गदर्शन करेगा।

आपके नए कौशल आपको अपने परिवेश में शीर्ष विशेषज्ञ बना देंगे”

सामान्य कौशल

- डेटा विश्लेषण के तकनीकी और व्यावसायिक परिप्रेक्ष्य विकसित करें
- डेटा की खोज, विज़ुअलाइज़ेशन, हेरफेर, प्रसंस्करण और विश्लेषण के लिए सबसे मौजूदा एल्गोरिदम, प्लेटफ़ॉर्म और टूल को समझें
- निर्णय लेने के लिए एक प्रमुख तत्व के रूप में मूल्य सृजन के लिए आवश्यक व्यावसायिक दृष्टिकोण लागू करें
- डेटा विश्लेषण के लिए विशिष्ट समस्याओं को संबोधित करने में सक्षम हों
- साइबर सुरक्षा में उपयोग की जाने वाली प्रणाली को जानें करें
- प्रत्येक मामले में इष्टतम समाधान पेश करने के लिए प्रत्येक प्रकार के खतरे का मूल्यांकन करें
- घटना व्यवहार को स्वचालित करने के लिए पूर्ण बुद्धिमान समाधान तैयार करें
- जानें कि कंपनी के बाहर और अंदर दोनों जगह कमजोरियों से जुड़े जोखिमों का आकलन कैसे किया जाए
- समय के साथ IoT के विकास और प्रभाव को समझें
- प्रदर्शित करें कि एक प्रणाली असुरक्षित है, निवारक उद्देश्यों के लिए उस पर हमला करें और उन समस्याओं का समाधान करें
- विभिन्न वातावरणों में सैंडबॉक्सिंग लागू करें
- उन दिशानिर्देशों को जानें जिनका एक अच्छे डेवलपर को आवश्यक सुरक्षा आवश्यकताओं का अनुपालन करने के लिए पालन करना चाहिए

विशिष्ट कौशल

- तकनीकी और व्यावसायिक दृष्टिकोण से डेटा साइंस में विशेषज्ञ
- विभिन्न प्रोफ़ाइलों द्वारा डेटा साझाकरण और समझ को बढ़ावा देने के लिए डेटा को सबसे उपयुक्त तरीके से विज़ुअलाइज़ करें
- संस्था के प्रमुख कार्यात्मक क्षेत्रों को संबोधित करें जहां डेटा साइंस सबसे अधिक मूल्य प्रदान कर सकता है
- डेटा जीवन चक्र, इसकी टाइपोलॉजी और इसके प्रबंधन के लिए आवश्यक प्रौद्योगिकियों और चरणों विकसित करें
- विशिष्ट भाषाओं और पुस्तकालयों का उपयोग करके डेटा को संसाधित और हेरफेर करें
- डेटा चयन, पूर्वप्रसंस्करण और परिवर्तन के लिए मौलिक डेटा माइनिंग तकनीकों में उन्नत ज्ञान विकसित करें
- डेटा में छिपे हुए ज्ञान के निष्कर्षण के लिए मुख्य मशीन लर्निंग एल्गोरिदम में विशेषज्ञ
- गहन डेटा उपयोग के लिए आवश्यक सॉफ्टवेयर वास्तुकला और प्रणाली में विशेष ज्ञान उत्पन्न करें
- निर्धारित करें कि आईओटी डेटा उत्पादन का स्रोत कैसे हो सकता है और ज्ञान निष्कर्षण के लिए डेटा साइंस को लागू करने के लिए महत्वपूर्ण जानकारी
- वास्तविक उदाहरणों से सीखकर विभिन्न क्षेत्रों या ऊर्ध्वाधर में डेटा साइंस को लागू करने के विभिन्न तरीकों का विश्लेषण करें
- रक्षात्मक सुरक्षा संचालन करें
- IT सुरक्षा के बारे में गहन और विशिष्ट धारणा रखें
- साइबर सुरक्षा और साइबर इंटेलिजेंस के क्षेत्र में विशेष ज्ञान रखें
- खुफिया चक्र, खुफिया स्रोत, सोशल इंजीनियरिंग, OSINT पद्धति, HUMINT, गुमनामीकरण और जोखिम विश्लेषण, मौजूदा प्रणाली (OWASP, OWISAM, OSSTM, PTES) और वर्तमान साइबर सुरक्षा नियमों जैसे मूलभूत पहलुओं का गहन ज्ञान रखें
- एक बहु-परत रक्षा तैयार करने के महत्व को समझें, जिसे गहराई से रक्षा के रूप में भी जाना जाता है, एक कॉर्पोरेट नेटवर्क के सभी पहलुओं को कवर करता है जहां कुछ अवधारणाओं और प्रणालियों को हम देखेंगे जिनका उपयोग घरेलू वातावरण में भी किया जा सकता है और लागू किया जा सकता है
- जानें कि स्मार्टफ़ोन और पोर्टेबल उपकरणों के लिए सुरक्षा प्रक्रियाएं कैसे लागू करें
- तथाकथित एथिकल हैकिंग करने और किसी कंपनी को साइबर हमले से बचाने के तरीकों को जानें
- साइबर सुरक्षा घटना की जाँच करें
- उपलब्ध विभिन्न आक्रमण और रक्षा तकनीकों को जानें
- साइबर सुरक्षा विश्लेषक की भूमिका का विश्लेषण करें और जानें कि सोशल इंजीनियरिंग कैसे काम करती है और इसके तरीके क्या हैं

> क्या आप खुद को अन्य विशेषज्ञों से अलग करना चाहते हैं, लेकिन नहीं जानते कि कैसे? यह उच्च स्नातकोत्तर उपाधि वह है जिसकी आप तलाश कर रहे हैं”

04

पाठ्यक्रम संचालन

यह उपाधि साइबर सुरक्षा और डिजिटल डेटा प्रबंधन के क्षेत्र में सर्वश्रेष्ठ प्रोफेसरों द्वारा पढ़ाई जाती है। उनका अनुभव इस बात की गारंटी देता है कि छात्रों को सबसे संपूर्ण और अद्यतित सामग्री तक पहुंच प्राप्त होगी ताकि वे इसे सीधे अपने पेशेवर करियर में लागू कर सकें। इस तरह, सुरक्षित सूचना प्रबंधन में इस उच्च स्नातकोत्तर उपाधि के शिक्षक अपना सारा ज्ञान छात्रों तक पहुंचाएंगे, यह सुनिश्चित करते हुए कि वे उच्च योग्य विशेषज्ञ बनें जिनकी उनके देशों में बड़ी कंपनियों द्वारा अत्यधिक मांग है।

सर्वश्रेष्ठ विशेषज्ञ आपको सिखाते हैं कि इस क्षेत्र में उत्कृष्ट पेशेवर कैसे बनें”

निर्देशन

डॉ. मार्टिन मार्टिन, आर्टुरो

- प्रोमेटियस ग्लोबल सॉल्यूशंस में सीईओ और सीटीओ
- कॉर्पोरेट टेक्नोलॉजीज में सीटीओ एन कॉर्पोरेट टेक्नोलॉजीज
- एआई शेफर्स जीएमबीएच में सीटीओ
- कैस्टिला ला मंचा विश्वविद्यालय से मनोविज्ञान में डॉक्टरेट
- कैमिलो जोस सेला विश्वविद्यालय से अर्थशास्त्र, व्यवसाय और वित्त में पीएचडी। डॉक्टरेट में उत्कृष्ट पुरस्कार
- कैस्टिला ला मंचा विश्वविद्यालय से मनोविज्ञान में डॉक्टरेट
- कैस्टिला विश्वविद्यालय से उन्नत सूचना प्रौद्योगिकी में स्नातकोत्तर उपाधि ला मंच
- कैस्टिला ला मंचा विश्वविद्यालय से उपाधि एमबीए+ई (बिजनेस एडमिनिस्ट्रेशन और संस्थानात्मक इंजीनियरिंग में स्नातकोत्तर उपाधि)
- एसोसिएट लेक्चरर, कैस्टिला ला मंचा विश्वविद्यालय में कंप्यूटर इंजीनियरिंग में स्नातक और स्नातकोत्तर उपाधि पढ़ाते हैं
- वालेंसिया के अंतर्राष्ट्रीय विश्वविद्यालय में बिग डेटा और डेटा साइंस में स्नातकोत्तर उपाधि के प्रोफेसर
- उद्योग 4.0 में स्नातकोत्तर उपाधि के व्याख्याता और औद्योगिक डिजाइन और उत्पाद विकास में स्नातकोत्तर उपाधि
- कैस्टिला ला मंचा विश्वविद्यालय के स्माइल अनुसंधान समूह के सदस्य

सुश्री. फर्नांडीज सपेना, सोनिया

- कंप्यूटर सुरक्षा और एथिकल हैकिंग ट्रेनर, गेटाफे नेशनल रेफरेंस सेंटर फॉर इंफॉर्मेटिक्स एंड टेलीकम्युनिकेशंस मैड्रिड
- सर्टिफाइड ई-काउंसिल प्रशिक्षक, मैड्रिड
- निम्नलिखित सर्टिफिकेशन में प्रशिक्षक: EXIN एथिकल हैकिंग फाउंडेशन और EXIN साइबर और IT सुरक्षा फाउंडेशन। मैड्रिड
- व्यावसायिकता के निम्नलिखित सर्टिफिकेट के साथ CAM द्वारा मान्यता प्राप्त विशेषज्ञ प्रशिक्षक: कंप्यूटर सुरक्षा (IFCT0190), वॉयस और डेटा नेटवर्क प्रबंधन (IFCM0310), विभागीय नेटवर्क प्रशासन (IFCT0410), दूरसंचार नेटवर्क में अलार्म प्रबंधन (IFCM0410), वॉयस और डेटा नेटवर्क ऑपरेटर (IFCM0110), और इंटरनेट सेवा प्रशासन (IFCT0509)
- बाहरी सहयोगी, CSO/SSA (मुख्य सुरक्षा अधिकारी/वरिष्ठ सुरक्षा वास्तुकार) बेलिएरिक द्वीप समूह विश्वविद्यालय
- कंप्यूटर इंजीनियर अल्काला डे हेनारेस विश्वविद्यालय, मैड्रिड
- DevOps में स्नातकोत्तर उपाधि: डॉकर और कुबेरनेट्स। कैस-प्रशिक्षण, मैड्रिड
- Microsoft Azure सुरक्षा टेक्नोलोजी. ई-काउंसिल, मैड्रिड

प्रोफेसर

श्री. आर्मेरो फर्नांडीज, राफेल

- SDG ग्रुप में व्यापार इंटेलिजेंस सलाहकार
- Mi-GSO में डिजिटल इंजीनियर
- टौरैसिड S.A. में लॉजिस्टिक इंजीनियर
- आईएनडीआरए में गुणवत्ता प्रशिक्षु
- वालेंसिया के पॉलिटेक्निक विश्वविद्यालय से एयरोस्पेस इंजीनियरिंग में स्नातक
- अल्काला डी हेनरेस विश्वविद्यालय से व्यावसायिक विकास 4.0 में स्नातकोत्तर उपाधि

श्री. पेरिस मोरिलो, लुइस जेवियर

- कैपिटोल कंसल्टिंग में तकनीकी लीड
- HCL में वरिष्ठ तकनीकी लीड& डिलिवरी लीड सपोर्ट
- मिराई एडवाइजरी में एजाइल कोच और संचालन निदेशक
- डेवलपर, टीम लीड, स्क्रम मास्टर, ऐजल कोच, डॉकपाथ में उत्पाद प्रबंधक
- स्यूदाद रियल(UCLM) के ESI द्वारा कंप्यूटर साइंस में उच्च इंजीनियरिंग
- CEOE-स्पेनिश कॉन्फेडरेशन ऑफ बिजनेस ऑर्गेनाइजेशन द्वारा परियोजना प्रबंधन में स्नातकोत्तर
- स्टैनफोर्ड विश्वविद्यालय, मिशिगन विश्वविद्यालय, योनसेई विश्वविद्यालय, मैड्रिड के पॉलिटेक्निक विश्वविद्यालय आदि जैसे प्रसिद्ध विश्वविद्यालयों द्वारा पढ़ाए जाने वाले 50+ एमओओसी लिए जाते हैं

श्री. मोंटोरो मोंटारोसो, एंड्रेस

- कैस्टिला-ला मंच विश्वविद्यालय में स्माइल समूह में शोधकर्ता
- प्रोमेटियस ग्लोबल सॉल्यूशंस में डेटा वैज्ञानिक
- कैस्टिला-ला मंचा विश्वविद्यालय से कंप्यूटर इंजीनियरिंग में उपाधि कंप्यूटर साइंस में
- ग्रेनेडा विश्वविद्यालय से डेटा साइंस और कंप्यूटर इंजीनियरिंग में स्नातकोत्तर उपाधि

श्रीमती. फर्नांडीज मेलेंडेज़, गैलिना

- ADN मोबाइल समाधान में डेटा विश्लेषक
- ईटीएल प्रक्रियाएं, डेटा माइनिंग, डेटा विश्लेषण और विसुअलाईज़शन, KPI's, की स्थापना, डैशबोर्ड डिजाइन और कार्यान्वयन, प्रबंधन नियंत्रण
- एडीएन मोबाइल सॉल्यूशन-गिजोन-स्पेन आर विकास, एसक्यूएल प्रबंधन, अन्य
- पैटर्न निर्धारण, भविष्य कहनेवाला मॉडलिंग, मशीन लर्निंग
- बिजनेस एडमिनिस्ट्रेशन में स्नातक की डिग्री। अरागुआ-काराकास की बाइसेन्टेनियल विश्वविद्यालय
- योजना और सार्वजनिक वित्त में डिप्लोमा। वेनेजुएला स्कूलों स्कूल ऑफ प्लानिंग- स्कूल ऑफ फाइनेंस
- डेटा विश्लेषण और बिजनेस इंटेलिजेंस में व्यावसायिक स्नातकोत्तर उपाधि, विश्वविद्यालय ओविएडो
- बिजनेस एडमिनिस्ट्रेशन और प्रबंधन में एमबीए (यूरोपीय बिजनेस स्कूल, बार्सिलोना)
- बिग डेटा और बिजनेस इंटेलिजेंस में स्नातकोत्तर (बार्सिलोना, यूरोपीय बिजनेस स्कूल)

श्रीमती. पेड्राजस परबास, ऐलेना

- मैड्रिड में प्रबंधन समाधान में व्यापार विश्लेषक
- कॉर्डोबा विश्वविद्यालय में कंप्यूटर विज्ञान और संख्यात्मक विश्लेषण विभाग में शोधकर्ता
- सैंटियागो डे कॉम्पोस्टेला में इंटेलिजेंट प्रौद्योगिकीयों में अनुसंधान के लिए सिंगुलर सेंटर में शोधकर्ता
- कंप्यूटर इंजीनियरिंग में उपाधि, डेटा साइंस में स्नातकोत्तर उपाधि और कंप्यूटर इंजीनियरिंग(यूरोपीय बिजनेस स्कूल, बार्सिलोना)

श्रीमती. मार्टिनेज सेराटो, येसिका

- सिक्योरिटस सुरक्षा स्पेन में इलेक्ट्रॉनिक सुरक्षा उत्पाद तकनीशियन
- रिकोपिया टेक्नोलॉजीज में बिजनेस इंटेलिजेंस विश्लेषक (अल्काला डी हेनारेस)
- पॉलिटेक्निक स्कूल, अल्काला विश्वविद्यालय में इलेक्ट्रॉनिक संचार इंजीनियरिंग में उपाधि
- रिकोपिया टेक्नोलॉजीज (अल्काला डी हेनारेस) में वाणिज्यिक प्रबंधन सॉफ्टवेयर (सीआरएम, ईआरपी, इंट्रानेट), उत्पाद और प्रक्रियाओं पर नई भर्तियों को प्रशिक्षित करने के लिए जिम्मेदार
- अल्काला विश्वविद्यालय में कंप्यूटर कक्षाओं में शामिल नए छात्रवृत्ति धारकों को प्रशिक्षित करने के लिए जिम्मेदार
- कॉररएओस और टेलेग्राफोस (मैड्रिड) में प्रमुख लेखा एकीकरण के क्षेत्र में परियोजना प्रबंधक
- कंप्यूटर तकनीशियन-कंप्यूटर कक्षाओं के लिए जिम्मेदार ओटीईसी, अल्काला विश्वविद्यालय (अल्काला डी हेनारेस)
- ASALUMA एसोसिएशन में कंप्यूटर क्लासेस शिक्षक (अल्काला डे हेनारेस)
- OTEC, अल्काला विश्वविद्यालय (अल्काला डे हेनरेस) में कंप्यूटर तकनीशियन के रूप में प्रशिक्षण के लिए छात्रवृत्ति

श्री. फ़ोंडन अल्काल्डे, रूबेन

- वोडाफोन स्पेन में ग्राहक मूल्य प्रबंधन व्यवसाय विश्लेषक
- टेलीफ़ोनिका ग्लोबल सॉल्यूशंस के लिए एंटेल्जी में सेवा एकीकरण के प्रमुख
- ईडीएम इलेक्ट्रॉनिक्स पर क्लोन सर्वर के लिए ऑनलाइन खाता प्रबंधक
- वोडाफोन ग्लोबल एंटरप्राइज में दक्षिणी यूरोप के लिए बिजनेस विश्लेषक
- मैड्रिड के यूरोपीय विश्वविद्यालय से दूरसंचार इंजीनियर
- इंटरनेशनल विश्वविद्यालय ऑफ वालेंसिया से बिग डेटा और विश्लेषिकी में स्नातकोत्तर उपाधि

श्री. डियाज़ डियाज़-चिरोन, टोबियास

- कैस्टिला-ला मंचा विश्वविद्यालय की आर्को प्रयोगशाला में शोधकर्ता, कंप्यूटर वास्तुकला और नेटवर्क से संबंधित परियोजनाओं के लिए समर्पित एक समूह
- दूरसंचार क्षेत्र के लिए समर्पित कंपनी ब्लू टेलीकॉम में सलाहकार
- कैस्टिला-ला मंचा विश्वविद्यालय से कंप्यूटर इंजीनियरिंग में उपाधि:

श्री. टाटो सांचेज, राफेल

- इंद्रा सिस्टेमस एस.ए. में परियोजना प्रबंधन मैड्रिड में यातायात महानिदेशालय के यातायात नियंत्रण और प्रबंधन केंद्र पर निर्भर बुद्धिमान परिवहन प्रणालियों की स्थापना के लिए रखरखाव अनुबंध का प्रबंधन
- मैड्रिड में यातायात सामान्य निदेशालय के यातायात नियंत्रण और प्रबंधन केंद्र के लिए जिम्मेदार इंद्रा सिस्टेमस के तकनीकी निदेशक एस.ए.
- प्रणाली इंजीनियर ENA ट्राफिको एस.ए.यू
- पॉलिटेक्निक विश्वविद्यालय मैड्रिड से बिजली में औद्योगिक तकनीकी इंजीनियर
- मैड्रिड के यूरोपीय विश्वविद्यालय से स्वचालन और शल्य औद्योगिक में उपाधि
- पेशेवर सर्टिफिकेशन। SSCE0110. रोजगार के लिए व्यावसायिक प्रशिक्षण के लिए शिक्षण
- ला रियोजा के अंतर्राष्ट्रीय विश्वविद्यालय (यूएनआईआर) से उद्योग 4.0 में स्नातकोत्तर उपाधि

श्री. कैटाला बारबा, जोस फ्रांसिस्को

- MINISDEF में मध्य प्रबंधन। GOE III के अंतर्गत विभिन्न कार्य और जिम्मेदारियाँ, जैसे आंतरिक नेटवर्क का प्रशासन और घटना प्रबंधन, विभिन्न क्षेत्रों के लिए अनुकूलित कार्यक्रमों का विकास, नेटवर्क उपयोगकर्ताओं और सामान्य रूप से समूह कर्मियों के लिए प्रशिक्षण पाठ्यक्रम
- अलमुसेफ्स, वालेंसिया में स्थित फोर्ड फैक्ट्री में इलेक्ट्रॉनिक तकनीशियन, रोबोट प्रोग्रामिंग, PLC's, मरम्मत और रखरखाव
- इलेक्ट्रॉनिक तकनीशियन
- मोबाइल उपकरणों के लिए एप्लिकेशन के डेवलपर

श्री. जिमेनेज़ रामोस, अल्वारो

- कैपजेमिनी में सुरक्षा विश्लेषक
- एक्सियंस में साइबर सुरक्षा विश्लेषक L1
- एक्सियंस में साइबर सुरक्षा विश्लेषक L2
- SACYR S.A में साइबर सुरक्षा विश्लेषक
- मैड्रिड के पॉलिटेक्निक विश्वविद्यालय से एयरोस्पेस इंजीनियरिंग में उपाधि
- CICE से साइबर सुरक्षा और एथिकल हैकिंग में स्नातकोत्तर उपाधि
- ड्यूस्टो ट्रेनिंग द्वारा साइबर सुरक्षा में उच्च पाठ्यक्रम

सुश्री. मार्कोस सरबारो, विक्टोरिया एलिसिया

- B60 UK में मूल एंड्रॉइड मोबाइल एप्लिकेशन डेवलपर
- ग्राहक की साइट पर सुरक्षा अलार्म के वर्चुअलाइज्ड वातावरण के प्रबंधन, समन्वय और दस्तावेज़ीकरण के लिए विश्लेषक प्रोग्रामर
- ग्राहक की साइट पर एटीएम के लिए जावा एप्लिकेशन के विश्लेषक प्रोग्रामर
- ग्राहक की साइट पर हस्ताक्षर सत्यापन और दस्तावेज़ प्रबंधन अनुप्रयोग के लिए सॉफ्टवेयर डेवलपमेंट प्रोफेशनल
- उपकरण के स्थानांतरण और ग्राहक की साइट पर PDA मोबाइल उपकरणों के प्रबंधन, रखरखाव और प्रशिक्षण के लिए प्रणाली तकनीशियन
- कैटालोनिया के मुक्त विश्वविद्यालय से कंप्यूटर प्रणाली की तकनीकी इंजीनियरिंग (UOC)
- प्रोफेशनल स्कूल ऑफ न्यू टेक्नोलॉजीज CICE से कंप्यूटर सिक्योरिटी और एथिकल हैकिंग ऑफिशियल EC- काउंसिल और कॉम्पटिया में स्नातकोत्तर उपाधि

श्री. पेराल्टा अलोंसो, जॉन

- वकील/डीपीओ अल्टिया कंसल्टोर्स एस.ए
- व्यक्तिगत डेटा संरक्षण, साइबर सुरक्षा और आईसीटी कानून में मास्टर में व्याख्याता, बास्क देश विश्वविद्यालय (यूपीवी-ईएचयू)
- वकील/कानूनी सलाहकार, अरियागा एसोसिएडोस एसेसोरामिएंटो ज्यूरिडिको वाई इकोनोमिया, एस.एल.
- कानूनी सलाहकार/प्रशिक्षु पेशेवर कार्यालय: ऑस्कर पदुरा
- बास्क देश के सार्वजनिक विश्वविद्यालय से कानून में उपाधि
- डेटा संरक्षण आयोग, ईआईएस इनोवेटिव स्कूल में स्नातकोत्तर उपाधि
- बास्क देश के सार्वजनिक विश्वविद्यालय से कानून में स्नातकोत्तर
- सिविल लिटिगेशन प्रैक्टिस में स्नातकोत्तर, अंतर्राष्ट्रीय विश्वविद्यालय इसाबेल आई डी कैस्टिला

मिस्टर. रेडोंडो, जीसस सेरानो

- जूनियर फ्रंटएंड डेवलपर और जूनियर साइबर सुरक्षा तकनीशियन
- टेलीफ़ोनिका, मैड्रिड में फ्रंटएंड डेवलपर
- फ्रंटएंड के डेवलपर बेस्ट प्रो कंसल्टेंसी एसएल, मैड्रिड
- दूरसंचार उपकरण और सेवाएँ इंस्टॉलर ग्रुपो जेनर, कैस्टिला वाई लियोन
- दूरसंचार उपकरण और सेवाएँ इंस्टॉलर कॉम्यूनिकेशियन एसएल, कैस्टिला वाई लियोन
- कंप्यूटर सुरक्षा सीएफटीआईसी गेटाफे, मैड्रिड में सर्टिफिकेट
- सुपीरियर तकनीशियन दूरसंचार और कंप्यूटर प्रणाली आईईएस त्रिनिदाद अरोयो, पलेंसिया
- वरिष्ठ तकनीशियन एमवी और एलवी इलेक्ट्रोटेक्निकल इंस्टालेशन आईईएस त्रिनिदाद अरोयो, पलेंसिया
- रिवर्स इंजीनियरिंग, स्टेनोग्राफी, एन्क्रिप्शन एकेडेमिया हैकर इंसीबे (टैलेंटोस इंसीबे) में प्रशिक्षण

> इस क्षेत्र के अग्रणी पेशेवर आपको इस क्षेत्र में सबसे व्यापक ज्ञान प्रदान करने के लिए एक साथ आए हैं, ताकि आप सफलता की पूरी गारंटी के साथ विकास कर सकें"

05

संरचना और विषय वस्तु

सुरक्षित सूचना प्रबंधन में इस उन्नत स्नातकोत्तर उपाधि की सामग्री को पेशे की वर्तमान स्थिति के अनुसार डिजाइन किया गया है, ताकि छात्रों को सर्वोत्तम संभव ज्ञान प्राप्त हो और वे इसे अपने कार्य वातावरण में लागू कर सकें। इसलिए, इस डिग्री को बनाने वाले 20 मॉड्यूल में, छात्र डिजिटल डेटा और सूचना के प्रबंधन और सुरक्षा के बारे में सब कुछ सीखेंगे, और क्षेत्र में सच्चे विशेषज्ञ बनेंगे।

इससे बेहतर कोई कार्यक्रम नहीं है। यह उच्च स्नातकोत्तर उपाधि आपको इन क्षेत्रों में शीर्ष विशेषज्ञ बनने के लिए आवश्यक सभी चीजें प्रदान करती है"

मॉड्यूल 1. एक व्यावसायिक संस्था में डेटा विश्लेषिकी

1.1. व्यापार विश्लेषण
- 1.1.1. व्यापार विश्लेषण
- 1.1.2. डेटा संरचना
- 1.1.3. चरण और तत्व

1.2. एंटरप्राइज़ में डेटा विश्लेषिकी
- 1.2.1. विभागों द्वारा स्कोरकार्ड और केपीआई
- 1.2.2. परिचालन, रणनीतिक और सामरिक रिपोर्ट
- 1.2.3. प्रत्येक विभाग पर लागू डेटा विश्लेषिकी
  - 1.2.3.1. विपणन और संचार
  - 1.2.3.2. वाणिज्यिक
  - 1.2.3.3. ग्राहक सेवा
  - 1.2.3.4. क्रय
  - 1.2.3.5. प्रशासन।
  - 1.2.3.6. एचआर
  - 1.2.3.7. प्रोडक्शन
  - 1.2.3.8. आईटी

1.3. विपणन और संचार
- 1.3.1. मापने के लिए KPI, अनुप्रयोग और लाभ
- 1.3.2. विपणन प्रणाली और डेटा वेयरहाउस
- 1.3.3. विपणन में एक डेटा विश्लेषिकी फ्रेमवर्क का कार्यान्वयन
- 1.3.4. विपणन और संचार योजना
- 1.3.5. रणनीतियाँ, पूर्वानुमान और अभियान प्रबंधन

1.4. वाणिज्यिक और बिक्री
- 1.4.1. वाणिज्यिक क्षेत्र में डेटा विश्लेषिकी का योगदान
- 1.4.2. बिक्री विभाग की जरूरतें
- 1.4.3. बाजार अनुसंधान

1.5. ग्राहक सेवा
- 1.5.1. निष्ठा
- 1.5.2. व्यक्तिगत गुणवत्ता और भावनात्मक बुद्धिमत्ता
- 1.5.3. ग्राहकों की संतुष्टि

1.6. क्रय
- 1.6.1. बाजार अनुसंधान के लिए डेटा विश्लेषिकी
- 1.6.2. प्रतिस्पर्धी अध्ययन के लिए डेटा विश्लेषण
- 1.6.3. अन्य अनुप्रयोगों

1.7. प्रशासन।
- 1.7.1. प्रशासन विभाग की जरूरतें
- 1.7.2. डेटा वेयरहाउस और वित्तीय जोखिम विश्लेषण
- 1.7.3. डेटा वेयरहाउस और क्रेडिट जोखिम विश्लेषण

1.8. मानव संसाधन
- 1.8.1. एचआर और डेटा विश्लेषण के लाभ
- 1.8.2. एचआर विभाग में डेटा विश्लेषिकी उपकरणें
- 1.8.3. एचआर में डेटा विश्लेषण का अनुप्रयोग

1.9. प्रोडक्शन
- 1.9.1. एक उत्पादन विभाग में डेटा विश्लेषण
- 1.9.2. अनुप्रयोग
- 1.9.3. फ़ायदे

1.10. आईटी
- 1.10.1. आईटी विभाग
- 1.10.2. डेटा विश्लेषिकी और डिजिटल परिवर्तन
- 1.10.3. नवाचार और उत्पादकता

मॉड्यूल 2. डेटा प्रबंधन, डेटा हेरफेर और डेटा साइंस रिपोर्टिंग

2.1. सांख्यिकी। चर, सूची और अनुपात
- 2.1.1. आंकड़े
- 2.1.2. सांख्यिकीय आयाम
- 2.1.3. चर, सूची और अनुपात

2.2. डेटा टाइपोलॉजी
- 2.2.1. गुणात्मक
- 2.2.2. मात्रात्मक
- 2.2.3. लक्षण वर्णन और श्रेणियाँ

2.3. माप से डेटा का ज्ञान
- 2.3.1. केंद्रीकरण मापें
- 2.3.2. फैलाव के उपाय
- 2.3.3. सहसंबंध

2.4. रेखांकन से डेटा का ज्ञान
- 2.4.1. डेटा प्रकार द्वारा प्रदर्शित करें
- 2.4.2. ग्राफ़िक जानकारी की व्याख्या
- 2.4.3. आर के साथ ग्राफ़िक्स का अनुकूलन

2.5. संभाव्यता
- 2.5.1. संभाव्यता
- 2.5.2. संभाव्यता फ़ंक्शन
- 2.5.3. वितरण

2.6. डेटा संग्रह
- 2.6.1. डेटा संग्रह की प्रणाली
- 2.6.2. डेटा संग्रह उपकरणें
- 2.6.3. डेटा संग्रह चैनलें

2.7. डेटा की सफाई
- 2.7.1. डेटा सफाई के चरण
- 2.7.2. डेटा गुणवत्ता
- 2.7.3. डेटा हेरफेर (आर के साथ)

2.8. डेटा विश्लेषण, व्याख्या और परिणामों का मूल्यांकन
- 2.8.1. सांख्यिकीय उपाय
- 2.8.2. संबंध सूचकांक
- 2.8.3. डेटा माइनिंग

2.9. डेटा वेयरहाउस
- 2.9.1. अवयव
- 2.9.2. डिजाइन

2.10. डेटा उपलब्धता
- 2.10.1. पहुँच
- 2.10.2. उपयोग
- 2.10.3. सुरक्षा/ सैफ्टी

मॉड्यूल 3. डेटा साइंस की नींव के रूप में IoT उपकरणों और प्लेटफ़ॉर्म

3.1. इंटरनेट ऑफ़ थिंग्स
- 3.1.1. भविष्य का इंटरनेट, इंटरनेट ऑफ थिंग्स
- 3.1.2. औद्योगिक इंटरनेट कंसोर्टियम

3.2. संदर्भ की वास्तुकला
- 3.2.1. संदर्भ की वास्तुकला
- 3.2.2. परतें
- 3.2.3. अवयव

3.3. सेंसर और आई ओ टी उपकरणों
- 3.3.1. मूल घटक
- 3.3.2. सेंसर और एक्चुएटर

3.4. संचार और प्रोटोकॉल
- 3.4.1. प्रोटोकॉल ओ एस आई मॉडल
- 3.4.2. संचार प्रौद्योगिकी

3.5. आईओटी और आईआईओटी के लिए क्लाउड प्लेटफ़ॉर्म
- 3.5.1. सामान्य प्रयोजन प्लेटफार्म
- 3.5.2. औद्योगिक प्लेटफार्म
- 3.5.3. कोड प्लेटफ़ॉर्म खोलें

3.6. आईओटी प्लेटफ़ॉर्म पर डेटा प्रबंधन
- 3.6.1. डेटा प्रबंधन तंत्र डेटा खोलें
- 3.6.2. डेटा और विज़ुअलाइज़ेशन एक्सचेंज

3.7. आईओटी सुरक्षा
- 3.7.1. आवश्यकताएँ और सुरक्षा क्षेत्र
- 3.7.2. IIoT सुरक्षा की रणनीतियाँ

3.8. आईओटी के अनुप्रयोग
- 3.8.1. बुद्धिमान शहर
- 3.8.2. आरोग्य और स्वस्थता
- 3.8.3. स्मार्ट घर
- 3.8.4. अन्य अनुप्रयोगों

3.9. आईआईओटी के अनुप्रयोग
- 3.9.1. छलरचना
- 3.9.2. परिवहन
- 3.9.3. ऊर्जा
- 3.9.4. कृषि एवं पशुधन
- 3.9.5. अन्य क्षेत्र

3.10. उद्योग 4.0.
- 3.10.1. आईओआरटी (रोबोटिक्स चीजों का इंटरनेट)
- 3.10.2. उडी एडिटिव मैन्युफैक्चरिंग
- 3.10.3. बिग डेटा विश्लेषण

मॉड्यूल 4. डेटा विश्लेषण के लिए ग्राफिकल प्रतिनिधित्व

4.1. खोजपूर्ण विश्लेषण
- 4.1.1. सूचना विश्लेषण के लिए प्रतिनिधित्व
- 4.1.2. ग्राफिकल प्रतिनिधित्व का मूल्य
- 4.1.3. ग्राफिकल प्रतिनिधित्व के नए प्रतिमान

4.2. डेटा विज्ञान के लिए अनुकूलन
- 4.2.1. रंग रेंज और डिज़ाइन
- 4.2.2. ग्राफिक प्रतिनिधित्व में गेस्टाल्ट
- 4.2.3. बचने की गलतियाँ और युक्तियाँ

4.3. बुनियादी डेटा स्रोत
- 4.3.1. गुणवत्तापूर्ण प्रतिनिधित्व के लिए
- 4.3.2. मात्रा प्रतिनिधित्व के लिए
- 4.3.3. समय प्रतिनिधित्व के लिए

4.4. जटिल डेटा स्रोत
- 4.4.1. फ़ाइलें, सूचियाँ और डेटाबेस
- 4.4.2. मुक्त डेटा
- 4.4.3. सतत जनरेशन डेटा

4.5. ग्राफ़ के प्रकार
- 4.5.1. मूल प्रतिनिधित्व
- 4.5.2. ब्लॉकों में प्रतिनिधित्व
- 4.5.3. फैलाव विश्लेषण के लिए प्रतिनिधित्व
- 4.5.4. परिपत्र अभ्यावेदन
- 4.5.5. बुलबुला प्रतिनिधित्व
- 4.5.6. भौगोलिक प्रतिनिधित्व

4.6. विज़ुअलाइज़ेशन के प्रकार
  4.6.1. तुलनात्मक और संबंधपरक
  4.6.2. वितरण
  4.6.3. श्रेणीबद्ध
4.7. ग्राफ़िक प्रतिनिधित्व के साथ रिपोर्ट डिज़ाइन
  4.7.1. विपणन रिपोर्टों में ग्राफ़ का अनुप्रयोग
  4.7.2. स्कोरकार्ड और केपीआई में ग्राफ़ का अनुप्रयोग
  4.7.3. रणनीतिक योजनाओं में ग्राफ़ का अनुप्रयोग
  4.7.4. अन्य उपयोग: विज्ञान, स्वास्थ्य, व्यवसाय
4.8. ग्राफिक वर्णन
  4.8.1. ग्राफिक वर्णन
  4.8.2. विकास
  4.8.3. उपयोग
4.9. विज़ुअलाइज़ेशन के लिए उन्मुख उपकरण
  4.9.1. अग्रिम उपकरण
  4.9.2. ऑनलाइन सॉफ्टवेयर
  4.9.3. खुला स्रोत
4.10. डेटा विज़ुअलाइज़ेशन में नई प्रौद्योगिकियाँ
  4.10.1. वास्तविकता विजुअल प्रणाली
  4.10.2. वास्तविकता संवर्धन और सुधार प्रणालियाँ
  4.10.3. इंटेलिजेंट प्रणाली

मॉड्यूल 5. साइंस डेटा उपकरण

5.1. डेटा विज्ञान
  5.1.1. डेटा विज्ञान
  5.1.2. डेटा वैज्ञानिकों के लिए उच्च उपकरण
5.2. डेटा, सूचना और ज्ञान
  5.2.1. डेटा, सूचना और ज्ञान
  5.2.2. डेटा के प्रकार
  5.2.3. डेटा स्रोत
5.3. डेटा से सूचना तक
  5.3.1. डेटा विश्लेषण
  5.3.2. विश्लेषण के प्रकार
  5.3.3. डेटासेट से जानकारी निकालना
5.4. विज़ुअलाइज़ेशन के माध्यम से जानकारी निकालना
  5.4.1. एक विश्लेषण उपकरण के रूप में विज़ुअलाइज़ेशन
  5.4.2. विज़ुअलाइज़ेशन के तरीके
  5.4.3. डेटासेट का विज़ुअलाइज़ेशन
5.5. डेटा गुणवत्ता
  5.5.1. गुणवत्ता डेटा
  5.5.2. डेटा सफाई
  5.5.3. बुनियादी डेटा प्रोसेसिंग
5.6. डेटासेट
  5.6.1. डेटासेट संवर्धन
  5.6.2. आयामीता का अभिशाप
  5.6.3. हमारे डेटासेट का संशोधन
5.7. असंतुलित होना
  5.7.1. वर्ग असंतुलन
  5.7.2. असंतुलित शमन तकनीक
  5.7.3. डेटासेट को संतुलित करना
5.8. अप्रशिक्षित मॉडल
  5.8.1. पर्यवेक्षित लर्निंग
  5.8.2. तरीके
  5.8.3. अप्रशिक्षित मॉडल के साथ वर्गीकरण
5.9. पर्यवेक्षित मॉडल
  5.9.1. पर्यवेक्षित मॉडल
  5.9.2. तरीके
  5.9.3. पर्यवेक्षित मॉडल के साथ वर्गीकरण
5.10. उपकरण और अच्छे अभ्यास
  5.10.1. डेटा वैज्ञानिकों के लिए अच्छे अभ्यास
  5.10.2. सबसे अच्छा मॉडल
  5.10.3. उपयोगी उपकरण

मॉड्यूल 6. डेटा माइनिंग चयन, प्रसंस्करण और परिवर्तन

6.1. सांख्यिकीय अनुमान
- 6.1.1. वर्णनात्मक सांख्यिकी बनाम सांख्यिकीय अनुमान
- 6.1.2. पैरामीट्रिक प्रक्रियाएँ
- 6.1.3. गैर-पैरामीट्रिक प्रक्रियाएँ

6.2. खोजपूर्ण विश्लेषण
- 6.2.1. विवरणात्मक विश्लेषण
- 6.2.2. विसुअलाईज़शन
- 6.2.3. डेटा तैयारी

6.3. डेटा तैयारी
- 6.3.1. इंटीग्रेशन और डेटा सफाई
- 6.3.2. डेटा सामान्यीकरण
- 6.3.3. गुण परिवर्तन

6.4. लुप्त मूल्य
- 6.4.1. लुप्त मूल्यों का उपचार
- 6.4.2. अधिकतम संभावना प्रतिरूपण विधियाँ
- 6.4.3. मशीन लर्निंग का उपयोग कर गुम मूल्य प्रतिरूपण

6.5. डेटा शोर
- 6.5.1. शोर वर्ग और गुण
- 6.5.2. शोर फ़िल्टरिंग
- 6.5.3. शोर का प्रभाव

6.6. आयामीता का अभिशाप
- 6.6.1. ओवरसैंपलिंग
- 6.6.2. अवर
- 6.6.3. बहुआयामी डेटा कटौती

6.7. सतत से असतत गुण तक
- 6.7.1. सतत डेटा बनाम विवेकशील डेटा
- 6.7.2. विवेकाधीन प्रक्रिया

6.8. आंकड़ा
- 6.8.1. डेटा चयन
- 6.8.2. संभावनाएँ और चयन मानदंड
- 6.8.3. चयन के तरीके

6.9. उदाहरण चयन
- 6.9.1. उदाहरण चयन के लिए तरीके
- 6.9.2. प्रोटोटाइप चयन
- 6.9.3. उदाहरण चयन के लिए उन्नत तरीके

6.10. बड़े डेटा वातावरण में डेटा प्रोसेसिंग
- 6.10.1. बिग डेटा
- 6.10.2. क्लासिक प्रीप्रोसेसिंग बनाम विशाल
- 6.10.3. स्मार्ट डेटा

मॉड्यूल 7. संभाव्यता सिद्धांत का पूर्वानुमान और विश्लेषण

7.1. समय श्रृंखला
- 7.1.1. समय श्रृंखला
- 7.1.2. उपयोग एवं प्रयोज्यता
- 7.1.3. संबंधित केस अध्ययन

7.2. समय श्रृंखला
- 7.2.1. एसटी की प्रवृत्ति मौसमी
- 7.2.2. विशिष्ट विविधताएँ
- 7.2.3. अवशेष विश्लेषण

7.3. टाइपोलॉजी
- 7.3.1. अचल
- 7.3.2. गैर-स्टेशनरी
- 7.3.3. परिवर्तन और समायोजन

7.4. समय श्रृंखला के लिए योजनाएँ
- 7.4.1. योगात्मक योजना (मॉडल)
- 7.4.2. गुणन योजना (मॉडल)
- 7.4.3. मॉडल का प्रकार निर्धारित करने की प्रक्रियाएँ

7.5. बुनियादी पूर्वानुमान विधियाँ
- 7.5.1. मीडिया
- 7.5.2. अनुभवहीन
- 7.5.3. मौसमी अनुभवहीन
- 7.5.4. तरीकों की तुलना

7.6. अवशेष विश्लेषण
  7.6.1. ऑटो सहसंबंध
  7.6.2. अवशेष एसीएफ
  7.6.3. सहसंबंध परीक्षण
7.7. समय श्रृंखला के संदर्भ में प्रतिगमन
  7.7.1. एनोवा
  7.7.2. मूलतत्त्व
  7.7.3. वास्तविक उपयोगिता
7.8. भविष्यसूचक समय श्रृंखला मॉडल
  7.8.1. अरिमा
  7.8.2. घातांक सुगम करना
7.9. आर के साथ समय श्रृंखला हेरफेर और विश्लेषण
  7.9.1. डेटा तैयारी
  7.9.2. पैटर्न की पहचान
  7.9.3. मॉडल विश्लेषण
  7.9.4. भविष्यवाणी
7.10. आर के साथ संयुक्त ग्राफिकल विश्लेषण
  7.10.1. विशिष्ट स्थितियाँ
  7.10.2. सरल समस्याओं के समाधान के लिए व्यावहारिक अनुप्रयोग
  7.10.3. उच्च समस्याओं के समाधान के लिए व्यावहारिक अनुप्रयोग

मॉड्यूल 8. इंटेलिजेंट प्रणाली का डिजाइन और विकास

8.1. डेटा प्री-प्रोसेसिंग
  8.1.1. डेटा प्री-प्रोसेसिंग
  8.1.2. डेटा परिवर्तन
  8.1.3. डेटा माइनिंग
8.2. स्वचालित सीखना
  8.2.1. पर्यवेक्षित और अपर्यवेक्षित शिक्षण
  8.2.2. रिइंफ़ोर्समेंट लर्निंग
  8.2.3. अन्य शिक्षण प्रतिमान
8.3. वर्गीकरण एल्गोरिदम
  8.3.1. आगमनात्मक स्वचालित लर्निंग
  8.3.2. एसवीएम और केएनएन
  8.3.3. रैंकिंग के लिए मेट्रिक्स और स्कोर
8.4. प्रतिगमन एल्गोरिदम
  8.4.1. रेखीय प्रतिगमन, लॉजिस्टिक प्रतिगमन और गैर-रेखीय मॉडल
  8.4.2. अस्थायी श्रृंखला
  8.4.3. प्रतिगमन के लिए मेट्रिक्स और स्कोर
8.5. क्लस्टरिंग एल्गोरिदम
  8.5.1. पदानुक्रमित समूहन तकनीकें
  8.5.2. आंशिक समूहन तकनीकें
  8.5.3. क्लस्टरिंग के लिए मेट्रिक्स और स्कोर
8.6. एसोसिएशन नियम तकनीक
  8.6.1. नियम निष्कर्षण के तरीके
  8.6.2. एसोसिएशन नियम एल्गोरिदम के लिए मेट्रिक्स और स्कोर
8.7. उन्नत वर्गीकरण तकनीकें बहुवर्गीकरणकर्ता
  8.7.1. बैगिंग एल्गोरिदम
  8.7.2. "यादृच्छिक वन" वर्गीकरणकर्ता
  8.7.3. निर्णय वृक्षों के लिए "बूस्टिंग"।
8.8. संभाव्य ग्राफिकल मॉडल
  8.8.1. संभाव्य मॉडल
  8.8.2. बायेसियन नेटवर्क गुण, प्रतिनिधित्व और पैरामीटरीकरण
  8.8.3. अन्य संभाव्य ग्राफिकल मॉडल
8.9. तंत्रिका नेटवर्क
  8.9.1. कृत्रिम तंत्रिका नेटवर्क के साथ मशीन लर्निंग
  8.9.2. फीडफॉरवर्ड नेटवर्क
8.10. डीप लर्निंग
  8.10.1. डीप फीडफॉरवर्ड नेटवर्क
  8.10.2. संवादात्मक तंत्रिका नेटवर्क और अनुक्रम मॉडल
  8.10.3. डीप न्यूरल नेटवर्क को लागू करने के लिए उपकरण

मॉड्यूल 9. डेटा-सघन प्रणाली और वास्तुकला

9.1. बड़े डेटा अनुप्रयोगों के गैर-कार्यात्मक आवश्यकताएँ स्तंभ
- 9.1.1. विश्वसनीयता
- 9.1.2. अनुकूलन
- 9.1.3. रख-रखाव

9.2. डेटा मॉडल
- 9.2.1. संबंधपरक मॉडल
- 9.2.2. वृत्तचित्र मॉडल
- 9.2.3. नेटवर्कस् डेटा मॉडल

9.3. डेटाबेस डेटा संग्रहण और पुनर्प्राप्ति प्रबंधन
- 9.3.1. हैश इंडेक्स
- 9.3.2. संरचित लॉग संग्रहण
- 9.3.3. पेड़ बी

9.4. डेटा कोडिंग प्रारूप
- 9.4.1. विशिष्ट भाषा प्रारूप
- 9.4.2. मानकीकृत प्रारूप
- 9.4.3. बाइनरी कोडिंग प्रारूप
- 9.4.4. प्रक्रियाओं के बीच डेटा फ्लौस

9.5. प्रतिकृति
- 9.5.1. प्रतिकृति के उद्देश्य
- 9.5.2. प्रतिकृति मॉडल
- 9.5.3. प्रतिकृति के साथ समस्याएँ

9.6. वितरित लेनदेन
- 9.6.1. लेनदेन
- 9.6.2. वितरित लेनदेन के लिए प्रोटोकॉल
- 9.6.3. क्रमबद्ध लेनदेन

9.7. विभाजन
- 9.7.1. विभाजन के स्वरूप
- 9.7.2. माध्यमिक सूचकांक इंटरैक्शन और विभाजन
- 9.7.3. विभाजन पुनर्संतुलन

9.8. ऑफ़लाइन डेटा संसाधित करना
- 9.8.1. प्रचय संसाधन
- 9.8.2. वितरित फ़ाइल प्रणाली
- 9.8.3. मानचित्र छोटा करना

9.9. वास्तविक समय में डेटा प्रोसेसिंग
- 9.9.1. मैसेज ब्रोकर के प्रकार
- 9.9.2. डेटा फ्लौस के रूप में डेटाबेस का प्रतिनिधित्व
- 9.9.3. डेटा स्ट्रीम प्रोसेसिंग

9.10. उद्यम के व्यावहारिक अनुप्रयोग
- 9.10.1. पढ़ने में एकरूपता
- 9.10.2. डेटा के प्रति समग्र दृष्टिकोण
- 9.10.3. वितरित सेवा का स्केलिंग

मॉड्यूल 10. व्यावहारिक अनुप्रयोगव्यावसायिक क्षेत्रों में डेटा साइंस

10.1. स्वास्थ्य सेवा क्षेत्र
- 10.1.1. स्वास्थ्य सेवा क्षेत्र और डेटा विश्लेषण में एआई के निहितार्थ
- 10.1.2. अवसर और चुनौतियाँ

10.2. स्वास्थ्य सेवा क्षेत्र के जोखिम और प्रवृत्तियाँ
- 10.2.1. स्वास्थ्य सेवा क्षेत्र में उपयोग करें
- 10.2.2. एआई के उपयोग से संबंधित संभावित जोखिम

10.3. वित्तीय सेवाएँ
- 10.3.1. वित्तीय सेवाएँ सेवा क्षेत्र और डेटा विश्लेषण में एआई के निहितार्थ
- 10.3.2. वित्तीय सेवाओं का उपयोग
- 10.3.3. एआई के उपयोग से संबंधित संभावित जोखिम

10.4. खुदरा
- 10.4.1. खुदरा सेवा क्षेत्र और डेटा विश्लेषण में एआई के निहितार्थ
- 10.4.2. खुदरा में उपयोग करें
- 10.4.3. एआई के उपयोग से संबंधित संभावित जोखिम

10.5. उद्योग 4.0.
- 10.5.1. 4.0 उद्योग में एआई और डेटा विश्लेषण के निहितार्थ
- 10.5.2. 4.0 उद्योग में उपयोग करें

10.6. उद्योग 4.0 के जोखिम और प्रवृत्तियाँ
- 10.6.1. एआई के उपयोग से संबंधित संभावित जोखिम

10.7. लोक प्रशासन
- 10.7.1. लोक प्रशासन में एआई और डेटा विश्लेषण के निहितार्थ
- 10.7.2. लोक प्रशासन में उपयोग
- 10.7.3. एआई के उपयोग से संबंधित संभावित जोखिम

10.8. शैक्षिक
- 10.8.1. शिक्षा में एआई और डेटा विश्लेषण के निहितार्थ
- 10.8.2. एआई के उपयोग से संबंधित संभावित जोखिम

10.9. वानिकी और कृषि
- 10.9.1. खुदरा सेवा क्षेत्र और डेटा विश्लेषण में एआई के निहितार्थ
- 10.9.2. वानिकी एवं कृषि में उपयोग
- 10.9.3. एआई के उपयोग से संबंधित संभावित जोखिम

10.10. मानव संसाधन
- 10.10.1. मानव संसाधन प्रबंधन में एआई और डेटा विश्लेषण के निहितार्थ
- 10.10.2. व्यापार जगत में व्यावहारिक अनुप्रयोग
- 10.10.3. एआई के उपयोग से संबंधित संभावित जोखिम

मॉड्यूल 11. साइबरइंटेलिजेंस और साइबर सुरक्षा

11.1. साइबरइंटेलिजेंस
- 11.1.1. साइबरइंटेलिजेंस
  - 11.1.1.2. बुद्धिमत्ता
    - 11.1.1.2.1. बुद्धि का चक्र
  - 11.1.1.3. साइबरइंटेलिजेंस
  - 11.1.1.4. साइबरइंटेलिजेंस और साइबर सुरक्षा
- 11.1.2. खुफिया विश्लेषक
  - 11.1.2.1. खुफिया विश्लेषक की भूमिका
  - 11.1.2.2. मूल्यांकन गतिविधि में खुफिया विश्लेषक के पूर्वाग्रह

11.2. साइबर सुरक्षा
- 11.2.1. सुरक्षा परतें
- 11.2.2. साइबर खतरों की पहचान
  - 11.2.2.1. बाहरी खतरे
  - 11.2.2.2. आंतरिक खतरे
- 11.2.3. प्रतिकूल खतरे
  - 11.2.3.1. सोशल इंजीनियरिंग
  - 11.2.3.2. सामान्यतः प्रयुक्त विधियाँ

11.3. बुद्धिमत्ता तकनीक और उपकरण
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. लिनक्स वितरण और उपकरण
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. मूल्यांकन पद्धतियाँ
- 11.4.1. खुफिया विश्लेषण
- 11.4.2. प्राप्त जानकारी की संस्था तकनीक
- 11.4.3. सूचना स्रोतों की विश्वसनीयता और विश्वसनीयता
- 11.4.4. विश्लेषण पद्धतियाँ
- 11.4.5. खुफिया परिणामों की प्रस्तुति

11.5. लेखापरीक्षा और दस्तावेज़ीकरण
- 11.5.1. आईटी सुरक्षा का लेखापरीक्षा
- 11.5.2. ऑडिटिंग के लिए दस्तावेज़ीकरण और परमिट
- 11.5.3. ऑडिट के प्रकार
- 11.5.4. वितरणयोग्य
  - 11.5.4.1. तकनीकी प्रतिवेदन
  - 11.5.4.2. कार्यकारी रिपोर्ट

11.6. नेटवर्क में गुमनामी
- 11.6.1. गुमनामी का प्रयोग
- 11.6.2. गुमनामी तकनीक (प्रॉक्सी, वीपीएन)
- 11.6.3. टीओआर, फ्रीनेट और आईपी2 नेटवर्क

11.7. खतरे और सुरक्षा के प्रकार
- 11.7.1. खतरों के प्रकार
- 11.7.2. शारीरिक सुरक्षा
- 11.7.3. नेटवर्क में सुरक्षा
- 11.7.4. तार्किक सुरक्षा
- 11.7.5. वेब अनुप्रयोगों में सुरक्षा
- 11.7.6. मोबाइल उपकरणों में सुरक्षा

11.8. विनियम और अनुपालन
- 11.8.1. जीडीपीआर
- 11.8.2. साइबर सुरक्षा की राष्ट्रीय रणनीति 2011
- 11.8.3. ISO, 27000 परिवार
- 11.8.4. एनआईएसटी साइबर सुरक्षा ढांचा
- 11.8.5. सीआईपी
- 11.8.6. आईएसओ बिजनेस स्कूल 27032
- 11.8.7. बादल विनियम
- 11.8.8. सॉक्स
- 11.8.9. आईसीपी

11.9. जोखिम विश्लेषण और मेट्रिक्स
- 11.9.1. जोखिम का दायरा
- 11.9.2. संपत्ति
- 11.9.3. धमकियाँ
- 11.9.4. कमजोरियाँ
- 11.9.5. जोखिम का आकलन
- 11.9.6. जोखिम उपचार

11.10. महत्वपूर्ण साइबर सुरक्षा एजेंसियाँ
- 11.10.1. एनआईएसटी
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. उनासुर - प्रोसुर

मॉड्यूल 12. मेज़बान सुरक्षा

12.1. सुरक्षा प्रतिलिपियाँ
- 12.1.1. सुरक्षा प्रतियों के लिए रणनीतियाँ
- 12.1.2. विंडोज़ के लिए उपकरण
- 12.1.3. लिनक्स के लिए उपकरण
- 12.1.4. MacOS के लिए उपकरण

12.2. उपयोगकर्ता एंटीवायरस
- 12.2.1. एंटीवायरस के प्रकार
- 12.2.2. विंडोज़ के लिए एंटीवायरस
- 12.2.3. लिनक्स के लिए एंटीवायरस
- 12.2.4. MacOS के लिए एंटीवायरस
- 12.2.5. स्मार्टफ़ोन के लिए एंटीवायरस

12.3. घुसपैठ डिटेक्टर-एचआईडीएस
- 12.3.1. घुसपैठ का पता लगाने के तरीके
- 12.3.2. सागन
- 12.3.3. सहयोगी
- 12.3.4. राखुंटर

12.4. स्थानीय फ़ायरवॉल
- 12.4.1. विंडोज़ के लिए फ़ायरवॉल
- 12.4.2. लिनक्स के लिए फ़ायरवॉल
- 12.4.3. MacOS के लिए फ़ायरवॉल

12.5. पासवर्ड प्रबंधक
- 12.5.1. पासवर्ड
- 12.5.2. लास्ट पास
- 12.5.3. कीपास
- 12.5.4. चिपचिपा पासवर्ड
- 12.5.5. रोबोफार्म

12.6. फ़िशिंग डिटेक्टर
- 12.6.1. फ़िशिंग का मैन्युअल पता लगाना
- 12.6.2. एंटीफ़िशिंग उपकरण

12.7. स्पाइवेयर
- 12.7.1. परिहार तंत्र
- 12.7.2. एंटीस्पाइवेयर उपकरण

12.8. ट्रैकर्स
- 12.8.1. प्रणाली की सुरक्षा के उपाय
- 12.8.2. एंटी-ट्रैकिंग उपकरण

12.9. ईडीआर - अंतिम बिंदु का पता लगाना और प्रतिक्रिया
- 12.9.1. ईडीआर प्रणाली का व्यवहार
- 12.9.2. ईडीआर और एंटीवायरस के बीच अंतर
- 12.9.3. ईडीआर प्रणाली का भविष्य

12.10. सॉफ़्टवेयर इंस्टालेशन पर नियंत्रण
- 12.10.1. रिपॉजिटरी और सॉफ्टवेयर स्टोर
- 12.10.2. अनुमत या निषिद्ध सॉफ़्टवेयर की सूची
- 12.10.3. उन्नयन मानदंड
- 12.10.4. सॉफ़्टवेयर स्थापित करने के विशेषाधिकार

मॉड्यूल 13. नेटवर्क सुरक्षा (परिधि)

13.1. जांच प्रणाली और खतरे की रोकथाम
- 13.1.1. सुरक्षा घटनाओं की सामान्य रूपरेखा
- 13.1.2. वर्तमान रक्षा प्रणालियाँ: गहराई और एसओसी में रक्षा
- 13.1.3. वर्तमान नेटवर्क वास्तुकला
- 13.1.4. घटना का पता लगाने और रोकथाम के लिए उपकरणों के प्रकार
  - 13.1.4.1. नेटवर्क आधारित प्रणाली
  - 13.1.4.2. होस्ट आधारित प्रणाली
  - 13.1.4.3. केंद्रीकृत प्रणाली
- 13.1.5. इंस्टेंस/होस्ट, कंटेनर और सर्वर रहित संचार और डिस्कवरी

13.2. फ़ायरवॉल
- 13.2.1. फ़ायरवॉल के प्रकार
- 13.2.2. हमले और शमन
- 13.2.3. कर्नेल लिनक्स में सामान्य फ़ायरवॉल
  - 13.2.3.1. यूएफडब्ल्यू
  - 13.2.3.2. Nftables और Iptables
  - 13.2.3.3. फ़ायरवॉल
- 13.2.4. प्रणाली लॉग पर आधारित डिटेक्शन प्रणाली
  - 13.2.4.1. टीसीपी रैपर्स
  - 13.2.4.2. ब्लॉकहोस्ट और डेनिहोस्ट
  - 13.2.4.3. Fai2ban

13.3. जांच प्रणाली और घुसपैठ रोकथाम (आईडीएस/आईपीएस)
- 13.3.1. आईडीएस/आईपीएस पर हमले
- 13.3.2. आईडीएस/आईपीएस प्रणाली
  - 13.3.2.1. फक-फक करना
  - 13.3.2.2. Suricata

13.4. अगली पीढ़ी के फ़ायरवॉल (एनजीएफडब्ल्यू)
- 13.4.1. एनजीएफडब्ल्यू और पारंपरिक फ़ायरवॉल के बीच अंतर
- 13.4.2. मुख्य क्षमताएँ
- 13.4.3. वाणिज्यिक समाधान
- 13.4.4. क्लाउड सेवाओं के लिए फ़ायरवॉल
  - 13.4.4.1. वीपीसी क्लाउड वास्तुकला
  - 13.4.4.2. एसीएलएस क्लाउड
  - 13.4.4.3. सुरक्षा समूह

13.5. प्रतिनिधि
- 13.5.1. प्रतिनिधि के प्रकार
- 13.5.2. प्रतिनिधि उपयोग के फायदे और नुकसान

13.6. एंटीवायरस मोटर्स
- 13.6.1. मैलवेयर और आईओसी का सामान्य संदर्भ
- 13.6.2. एंटीवायरस मोटर्स की समस्याएं

13.7. मेल सुरक्षा प्रणालियाँ
- 13.7.1. स्पैम - विरोधी
  - 13.7.1.1. सफ़ेद और काली सूचियाँ
  - 13.7.1.2. बायेसियन फ़िल्टर
- 13.7.2. मेल गेटवे (एमजीडब्ल्यू)

13.8. सिएम
- 13.8.1. वास्तुकला और घटक
- 13.8.2. सहसंबंध नियम और उपयोग के मामले
- 13.8.3. सिएम प्रणाली की वर्तमान चुनौतियाँ

13.9. SOAR
- 13.9.1. SOAR और सिएम: शत्रु या सहयोगी
- 13.9.2. SOAR प्रणाली का भविष्य

13.10. अन्य नेटवर्क आधारित प्रणाली
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. हनीपोट्स और हनीनेट्स
- 13.10.4. CASB

मॉड्यूल 14. स्मार्टफ़ोन सुरक्षा

14.1. मोबाइल उपकरणों की दुनिया
- 14.1.1. मोबाइल प्लेटफ़ॉर्म के प्रकार
- 14.1.2. iOS उपकरणों
- 14.1.3. एंड्रॉइड उपकरणों

14.2. मोबाइल सुरक्षा का प्रबंधन
- 14.2.1. OWASP मोबाइल सुरक्षा परियोजना
  - 14.2.1.1. शीर्ष 10 कमजोरियाँ
- 14.2.2. संचार, नेटवर्क और कनेक्शन मोड

14.3. बिजनेस वर्ल्ड में मोबाइल उपकरणों
- 14.3.1. जोखिम
- 14.3.2. सुरक्षा नीतियाँ
- 14.3.3. उपकरणों की निगरानी
- 14.3.4. मोबाइल उपकरणों प्रबंधन (एमडीएम)

14.4. उपयोगकर्ता गोपनीयता और डेटा सुरक्षा
- 14.4.1. सूचना स्थितियाँ
- 14.4.2. डेटा की सुरक्षा और गोपनीयता
  - 14.4.2.1. लाइसेंस
  - 14.4.2.2. एन्क्रिप्शन
- 14.4.3. सुरक्षित डेटा संग्रहण
  - 14.4.3.1. सुरक्षित iOS संग्रहण
  - 14.4.3.2. सुरक्षित एंड्रॉइड स्टोरेज
- 14.4.4. अनुप्रयोग विकास में सर्वोत्तम अभ्यास

14.5. कमजोरियाँ और आक्रमण कारक
- 14.5.1. कमजोरियाँ
- 14.5.2. हमला वेक्टर
  - 14.5.2.1. मैलवेयर
  - 14.5.2.2. डेटा निष्कासन
  - 14.5.2.3. डेटा मेनिपुलेशन

14.6. मुख्य खतरे
- 14.6.1. जबरदस्ती उपयोगकर्ता
- 14.6.2. मैलवेयर
  - 14.6.2.1. मैलवेयर के प्रकार
- 14.6.3. सोशल इंजीनियरिंग
- 14.6.4. डेटा रिसाव
- 14.6.5. सूचना चोरी
- 14.6.6. असुरक्षित वाई-फ़ाई नेटवर्क
- 14.6.7. पुराना सॉफ्टवेयर
- 14.6.8. दुर्भावनापूर्ण अनुप्रयोग
- 14.6.9. असुरक्षित पासवर्ड
- 14.6.10. कमज़ोर विन्यास या अस्तित्वहीन सुरक्षा
- 14.6.11. भौतिक प्रवेश
- 14.6.12. उपकरणों की हानि या चोरी
- 14.6.13. पहचान की चोरी (अखंडता)
- 14.6.14. कमजोर या टूटी हुई क्रिप्टोग्राफी
- 14.6.15. सेवा से इनकार (DoS)

14.7. मुख्य हमले
- 14.7.1. फ़िशिंग हमले
- 14.7.2. संचार के तरीकों से संबंधित हमले
- 14.7.3. स्मिशिंग हमले
- 14.7.4. क्रिप्टोजैकिंग हमले
- 14.7.5. बीच वाला व्यक्ति

14.8. हैकिंग
- 14.8.1. रूटिंग और जेलब्रेकिंग
- 14.8.2. मोबाइल हमले की शारीरिक रचना
  - 14.8.2.1. ख़तरे का प्रचार
  - 14.8.2.2. उपकरणों पर मैलवेयर की स्थापना
  - 14.8.2.3. अटलता
  - 14.8.2.4. पेलोड निष्पादन और सूचना निष्कर्षण

14.8.3. iOS उपकरणों पर हैकिंग: तंत्र और उपकरण
14.8.4. एंड्रॉइड उपकरणों पर हैकिंग: तंत्र और उपकरण
14.9. भेदन परीक्षण
14.9.1. iOS पेनटेस्टिंग
14.9.2. एंड्रॉइड पेनटेस्टिंग
14.9.3. औजारें
14.10. संरक्षण और सुरक्षा
14.10.1. सुरक्षा विन्यास
14.10.1.1. iOS उपकरणों में
14.10.1.2. एंड्रॉइड उपकरणों में
14.10.2. सुरक्षा उपाय
14.10.3. सुरक्षा उपकरण

मॉड्यूल 15. आईओटी सुरक्षा

15.1. उपकरण
15.1.1. उपकरणों के प्रकार
15.1.2. मानकीकृत वास्तुकला
15.1.2.1. ONEM2M
15.1.2.2. IoTWF
15.1.3. अनुप्रयोग प्रोटोकॉल
15.1.4. कनेक्टिविटी टेक्नोलॉजीज
15.2. IoT उपकरण अनुप्रयोग क्षेत्र
15.2.1. स्मार्ट घर
15.2.2. स्मार्ट शहर
15.2.3. परिवहन
15.2.4. पहनने योग्य
15.2.5. स्वास्थ्य सेवा क्षेत्र
15.2.6. IioT
15.3. संचार प्रोटोकॉल
15.3.1. QTTM
15.3.2. LWM2M
15.3.3. OMA-DM
15.3.4. TR-069
15.4. स्मार्ट घर
15.4.1. घर स्वचालन
15.4.2. नेटवर्क्स्
15.4.3. इलेक्ट्रोडोमेस्टिक्स
15.4.4. निगरानी एवं सुरक्षा
15.5. स्मार्ट शहर
15.5.1. रोशनी
15.5.2. अंतरिक्ष-विज्ञान
15.5.3. सुरक्षा/ सैफ्टी
15.6. परिवहन
15.6.1. स्थानीयकरण
15.6.2. भुगतान करना और सेवाएँ प्राप्त करना
15.6.3. कनेक्टिविटी
15.7. पहनने योग्य
15.7.1. बुद्धिमान कपड़े
15.7.2. बुद्धिमान आभूषण
15.7.3. बुद्धिमान घड़ियाँ
15.8. स्वास्थ्य सेवा क्षेत्र
15.8.1. व्यायाम निगरानी/हृदय ताल
15.8.2. मरीजों और बुजुर्ग लोगों की निगरानी
15.8.3. प्रत्यारोपण
15.8.4. सर्जिकल रोबोट
15.9. कनेक्टिविटी
15.9.1. वाई-फ़ाई/गेटवे
15.9.2. ब्लूटूथ
15.9.3. सम्मिलित कनेक्टिविटी
15.10. प्रतिभूतिकरण
15.10.1. समर्पित नेटवर्क
15.10.2. पासवर्ड प्रबंधक
15.10.3. एन्क्रिप्टेड प्रोटोकॉल का उपयोग
15.10.4. युक्तियों का प्रयोग करें

मॉड्यूल 16. नैतिक हैकिंग

16.1. काम का माहौल
- 16.1.1. लिनक्स वितरण
  - 16.1.1.1. काली लिनक्स - आक्रामक सुरक्षा
  - 16.1.1.2. तोता ओएस
  - 16.1.1.3. उबंटू
- 16.1.2. वर्चुअलाइजेशन प्रणाली
- 16.1.3. सैंडबॉक्स
- 16.1.4. प्रयोगशालाओं की तैनाती

16.2. तरीके
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. एनआईएसटी
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. फूटप्रिन्टिंग
- 16.3.1. ओपन-सोर्स इंटेलिजेंस (OSINT)
- 16.3.2. डेटा उल्लंघनों और कमजोरियों की खोज करें
- 16.3.3. निष्क्रिय उपकरणों का उपयोग

16.4. नेटवर्क स्कैनिंग
- 16.4.1. स्कैनिंग उपकरण
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. अन्य स्कैनिंग उपकरण
- 16.4.2. स्कैनिंग तकनीक
- 16.4.3. फ़ायरवॉल एल और आईडीएस चोरी तकनीक
- 16.4.4. बैनर हथियाना
- 16.4.5. नेटवर्क आरेख

16.5. गणना
- 16.5.1. एसएमटीपी गणना
- 16.5.2. डीएनएस गणना
- 16.5.3. NetBIOS और सांबा गणना
- 16.5.4. एलडीएपी गणना
- 16.5.5. एसएनएमपी गणना
- 16.5.6. गणना की अन्य तकनीकें

16.6. भेद्यता विश्लेषण
- 16.6.1. भेद्यता स्कैनिंग समाधान
  - 16.6.1.1. क्वालिस
  - 16.6.1.2. नेसस
  - 16.6.1.3. सीएफआई लैनगार्ड
- 16.6.2. भेद्यता स्कोरिंग प्रणाली
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. वायरलेस नेटवर्क पर हमले
- 16.7.1. वायरलेस नेटवर्क की हैकिंग पद्धति
  - 16.7.1.1. वाई-फाई डिस्कवरी
  - 16.7.1.2. यातायात विश्लेषण
  - 16.7.1.3. हवाई हमले
    - 16.7.1.3.1. WEP हमले
    - 16.7.1.3.2. WPA/WPA2 हमले
  - 16.7.1.4. दुष्ट जुड़वां हमले
  - 16.7.1.5. WPS हमले
  - 16.7.1.6. धक्का
- 16.7.2. वायरलेस सुरक्षा के लिए उपकरण

16.8. वेब सर्वर की हैकिंग
- 16.8.1. क्रॉस साइट स्क्रिप्टिंग
- 16.8.2. CSRF
- 16.8.3. अपहरण सत्र
- 16.8.4. एसक्यूएल इंजेक्शन

16.9. कमजोरियों का शोषण
- 16.9.1. ज्ञात कारनामों का उपयोग
- 16.9.2. ज्ञात मेटास्प्लोइट का उपयोग
- 16.9.3. मैलवेयर का उपयोग
  - 16.9.3.1. परिभाषा और दायरा
  - 16.9.3.2. मैलवेयर जेनरेशन
  - 16.9.3.3. एंटीवायरस समाधानों को बायपास करना

16.10. अटलता
- 16.10.1. रूटकिट्स इंस्टालेशन
- 16.10.2. एनकैट का उपयोग
- 16.10.3. बैकडोर के लिए निर्धारित कार्यों का उपयोग
- 16.10.4. उपयोगकर्ता निर्माण
- 16.10.5. HIDS खोज

मॉड्यूल 17. रिवर्स इंजीनियरिंग

17.1. संकलनकर्ता
- 17.1.1. कोड के प्रकार
- 17.1.2. एक कंपाइलर के लिए चरण
- 17.1.3. प्रतीकों की तालिका
- 17.1.4. गलती प्रबंधक
- 17.1.5. जीसीसी कंपाइलर

17.2. कंपाइलर्स में विश्लेषण के प्रकार
- 17.2.1. शाब्दिक विश्लेषण
  - 17.2.1.1. शब्दावली।
  - 17.2.1.2. शाब्दिक घटक
  - 17.2.1.3. लेक्स लेक्सिकल विश्लेषक
- 17.2.2. वाक्यात्मक विश्लेषण
  - 17.2.2.1. प्रसंग-मुक्त व्याकरण
  - 17.2.2.2. वाक्यात्मक विश्लेषण के प्रकार
    - 17.2.2.2.1. ऊपर से नीचे तक विश्लेषण
    - 17.2.2.2.2. बॉटम-अप विश्लेषण
  - 17.2.2.3. वाक्यात्मक वृक्ष और व्युत्पत्तियाँ
  - 17.2.2.4. सिंटैक्टिक एनालाइजर के प्रकार
    - 17.2.2.4.1. एलआर विश्लेषक (बाएं से दाएं)
    - 17.2.2.4.2. एलएएलआर विश्लेषक
- 17.2.3. सिमेंटिक विश्लेषण
  - 17.2.3.1. गुण व्याकरण
  - 17.2.3.2. एस-जिम्मेदार
  - 17.2.3.3. एल-जिम्मेदार

17.3. असेंबलर में डेटा संरचनाएँ
- 17.3.1. वेरिएबल्स
- 17.3.2. सरणियों
- 17.3.3. संकेत
- 17.3.4. संरचनाएँ
- 17.3.5. ओब्जेक्ट्स

17.4. असेंबलर कोड संरचनाएँ
- 17.4.1. चयन संरचनाएँ
  - 17.4.1.1. यदि, अन्यथा यदि, अन्यथा
  - 17.4.1.2. बदलना
- 17.4.2. पुनरावृत्ति संरचनाएँ
  - 17.4.2.1. के लिए
  - 17.4.2.2. जबकि
  - 17.4.2.3. ब्रेक का उपयोग
- 17.4.3. कार्य

17.5. X86 हार्डवेयर वास्तुकला
- 17.5.1. x86 प्रोसेसर वास्तुकला
- 17.5.2. X86 डेटा संरचनाएँ
- 17.5.3. x86 कोड संरचनाएँ

17.6. एआरएम हार्डवेयर वास्तुकला
- 17.6.1. एआरएम प्रोसेसर वास्तुकला
- 17.6.2. एआरएम डेटा संरचनाएँ
- 17.6.3. एआरएम कोड संरचनाएँ

17.7. स्थैतिक कोड विश्लेषण
- 17.7.1. जुदा करने वाले
- 17.7.2. IDA
- 17.7.3. कोड पुनर्निर्माणकर्ता

17.8. डायनेमिक्स कोड विश्लेषण
- 17.8.1. क्रय व्यवहार विश्लेषण
  - 17.8.1.1. संचार
  - 17.8.1.2. मॉनिटरिंग
- 17.8.2. लिनक्स कोड डिबगर्स
- 17.8.3. विंडोज़ कोड डिबगर्स

17.9. सैंडबॉक्स
- 17.9.1. सैंडबॉक्स वास्तुकला
- 17.9.2. सैंडबॉक्स से बचाव
- 17.9.3. पता लगाने की तकनीक
- 17.9.4. बचने की तकनीकें
- 17.9.5. जवाबीउपाय
- 17.9.6. लिनक्स में सैंडबॉक्स
- 17.9.7. विंडोज़ में सैंडबॉक्स
- 17.9.8. MacOS में सैंडॉक्स
- 17.9.9. एंड्रॉइड में सैंडबॉक्स

17.10. मैलवेयर विश्लेषण
- 17.10.1. मैलवेयर के विश्लेषण के तरीके
- 17.10.2. मैलवेयर अस्पष्टीकरण तकनीकें
  - 17.10.2.1. निष्पादन योग्य अस्पष्टता
  - 17.10.2.2. निष्पादन वातावरण का प्रतिबंध
- 17.10.3. मैलवेयर विश्लेषण उपकरण

मॉड्यूल 18. सुरक्षित विकास

18.1. सुरक्षित विकास
- 18.1.1. गुणवत्ता, कार्यक्षमता और सुरक्षा
- 18.1.2. गोपनीयता, सत्यनिष्ठा और उपलब्धता
- 18.1.3. सॉफ्टवेयर विकास जीवन चक्र

18.2. आवश्यकताएँ चरण
- 18.2.1. प्रमाणीकरण नियंत्रण
- 18.2.2. भूमिका और विशेषाधिकार नियंत्रण
- 18.2.3. जोखिम-उन्मुख आवश्यकताएँ
- 18.2.4. विशेषाधिकार अनुमोदन

18.3. विश्लेषण और डिज़ाइन चरण
- 18.3.1. घटक पहुंच और प्रणाली प्रशासन
- 18.3.2. ऑडिट ट्रैल्स
- 18.3.3. सत्र प्रबंधन
- 18.3.4. ऐतिहासिक डेटा
- 18.3.5. उचित त्रुटि प्रबंधन
- 18.3.6. कार्यों का पृथक्करण

18.4. कार्यान्वयन और कोडिंग चरण
- 18.4.1. विकास वातावरण सुनिश्चित करना
- 18.4.2. तकनीकी दस्तावेज़ीकरण की तैयारी
- 18.4.3. सुरक्षित कोडिंग
- 18.4.4. संचार सुरक्षा

18.5. सुरक्षित कोडिंग की अच्छी प्रथाएँ
- 18.5.1. प्रवेश डेटा का सत्यापन
- 18.5.2. आउटपुट डेटा की कोडिंग
- 18.5.3. प्रोग्रामिंग शैली
- 18.5.4. लॉग प्रबंधन बदलें
- 18.5.5. क्रिप्टोग्राफ़िक प्रथाएँ
- 18.5.6. गलतियों और लॉग का प्रबंधन
- 18.5.7. फ़ाइल प्रबंधन
- 18.5.8. स्मृति प्रबंधन
- 18.5.9. सुरक्षा कार्यों का मानकीकरण और पुन: उपयोग

18.6. सर्वर की तैयारी और हार्डनिंग
- 18.6.1. सर्वर पर उपयोगकर्ताओं, समूहों और भूमिकाओं का प्रबंधन
- 18.6.2. सॉफ्टवेयर स्थापना
- 18.6.3. सर्वर हार्डनिंग
- 18.6.4. अनुप्रयोग परिवेश का मजबूत विन्यास

18.7. डीबी तैयारी और हार्डनिंग
- 18.7.1. डीबी इंजन अनुकूलन
- 18.7.2. एप्लिकेशन के लिए अपना स्वयं का उपयोगकर्ता बनाएँ
- 18.7.3. उपयोगकर्ता को आवश्यक विशेषाधिकार सौंपना
- 18.7.4. डीबी का सख्त होना

18.8. परीक्षण चरण
- 18.8.1. सुरक्षा नियंत्रण में गुणवत्ता नियंत्रण
- 18.8.2. चरणबद्ध कोड निरीक्षण
- 18.8.3. विन्यास प्रबंधन की जाँच करना
- 18.8.4. ब्लैक बॉक्स परीक्षण

18.9. उत्पादन में परिवर्तन की तैयारी
- 18.9.1. परिवर्तन नियंत्रण निष्पादित करें
- 18.9.2. उत्पादन परिवर्तन प्रक्रिया को पूरा करें
- 18.9.3. रोलबैक प्रक्रिया निष्पादित करें
- 18.9.4. प्री-प्रोडक्शन परीक्षण

18.10. रखरखाव चरण
- 18.10.1. जोखिम-आधारित आश्वासन
- 18.10.2. व्हाइट बॉक्स सुरक्षा रखरखाव परीक्षण
- 18.10.3. ब्लैक बॉक्स सुरक्षा रखरखाव परीक्षण

मॉड्यूल 19. फोरेंसिक विश्लेषण

19.1. डेटा अधिग्रहण और दोहराव
- 19.1.1. अस्थिर डेटा अधिग्रहण
  - 19.1.1.1. व्यवस्था जानकारी
  - 19.1.1.2. नेटवर्क जानकारी
  - 19.1.1.3. अस्थिरता क्रम
- 19.1.2. स्थैतिक डेटा अधिग्रहण
  - 19.1.2.1. डुप्लिकेट छवि बनाना
  - 19.1.2.2. हिरासत दस्तावेज़ की एक श्रृंखला तैयार करना
- 19.1.3. प्राप्त डेटा के सत्यापन के लिए तरीके
  - 19.1.3.1. लिनक्स के लिए तरीके
  - 19.1.3.2. विंडोज़ के लिए तरीके

19.2. एंटीफोरेंसिक तकनीकों का मूल्यांकन और हार
- 19.2.1. एंटीफोरेंसिक तकनीकों के उद्देश्य
- 19.2.2. डेटा हटाना
  - 19.2.2.1. डेटा हटाना और फ़ाइलें
  - 19.2.2.2. फ़ाइल रिकवरी
  - 19.2.2.3. हटाए गए विभाजनों की पुनर्प्राप्ति
- 19.2.3. पासवर्ड सुरक्षा
- 19.2.4. स्टेग्नोग्राफ़ी
- 19.2.5. सुरक्षित डिवाइस वाइपिंग
- 19.2.6. एन्क्रिप्शन

19.3. ऑपरेटिंग प्रणाली का फोरेंसिक विश्लेषण
- 19.3.1. विंडोज़ फोरेंसिक विश्लेषण
- 19.3.2. लिनक्स फोरेंसिक विश्लेषण
- 19.3.3. मैक फोरेंसिक विश्लेषण

19.4. नेटवर्क फोरेंसिक विश्लेषण
- 19.4.1. लॉग विश्लेषण
- 19.4.2. डेटा का सहसंबंध
- 19.4.3. नेटवर्क जांच
- 19.4.4. नेटवर्क फोरेंसिक विश्लेषण में अनुसरण करने योग्य चरण

19.5. वेब फोरेंसिक विश्लेषण
- 19.5.1. वेब हमलों की जांच
- 19.5.2. हमले का पता लगाना
- 19.5.3. आईपी पता स्थान

19.6. डेटाबेस का फोरेंसिक विश्लेषण
- 19.6.1. एMSSQL फोरेंसिक विश्लेषण
- 19.6.2. MySQL फोरेंसिक विश्लेषण
- 19.6.3. PostgreSQL फोरेंसिक विश्लेषण
- 19.6.4. MongoDB फोरेंसिक विश्लेषण

19.7. क्लाउड फोरेंसिक विश्लेषण
- 19.7.1. क्लाउड में अपराधों के प्रकार
  - 19.7.1.1. विषय के रूप में क्लाउड
  - 19.7.1.2. वस्तु के रूप में क्लाउड
  - 19.7.1.3. उपकरण के रूप में क्लाउड
- 19.7.2. क्लाउड फोरेंसिक की चुनौतियाँ
- 19.7.3. क्लाउड में भंडारण सेवाओं की जांच
- 19.7.4. क्लाउड के लिए फोरेंसिक विश्लेषण उपकरण

19.8. ईमेल अपराधों की जांच
- 19.8.1. मेल प्रणाली
  - 19.8.1.1. मेल ग्राहक
  - 19.8.1.2. सर्वर ग्राहक
  - 19.8.1.3. SMTP सर्वर
  - 19.8.1.4. POP3 सर्वर
  - 19.8.1.5. IMAP4 सर्वर
- 19.8.2. मेल अपराध
- 19.8.3. मेल संदेश
  - 19.8.3.1. मानक शीर्षलेख
  - 19.8.3.2. विस्तारित शीर्षलेख
- 19.8.4. इन अपराधों की जांच के लिए कदम
- 19.8.5. ईमेल के लिए फोरेंसिक उपकरण

19.9. मोबाइलों का फोरेंसिक विश्लेषण
- 19.9.1. सेलुलर नेटवर्क
  - 19.9.1.1. नेटवर्क के प्रकार
  - 19.9.1.2. CDR सामग्री
- 19.9.2. सब्सक्राइबर आइडेंटिटी मॉड्यूल (सिम)
- 19.9.3. तार्किक अधिग्रहण
- 19.9.4. भौतिक अधिग्रहण
- 19.9.5. फ़ाइल प्रणाली अधिग्रहण

19.10. फोरेंसिक रिपोर्ट लेखन और प्रस्तुति
- 19.10.1. फोरेंसिक रिपोर्ट के महत्वपूर्ण पहलू
- 19.10.2. रिपोर्टों का वर्गीकरण और प्रकार
- 19.10.3. रिपोर्ट लिखने के लिए मार्गदर्शिका
- 19.10.4. रिपोर्ट प्रस्तुत करना
  - 19.10.4.1. गवाही देने के लिए पूर्व तैयारी
  - 19.10.4.2. निक्षेप
  - 19.10.4.3. मीडिया से निपटना

मॉड्यूल 20. IT सुरक्षा में वर्तमान और भविष्य की चुनौतियाँ

20.1. ब्लॉकचेन प्रौद्योगिकी
- 20.1.1. आवेदन की गुंजाइश
- 20.1.2. गोपनीयता की गारंटी
- 20.1.3. गैर-अस्वीकृति की गारंटी

20.2. डिजिटल मनी
- 20.2.1. बिटकोईन
- 20.2.2. क्रिप्टोकरेंसी
- 20.2.3. क्रिप्टोक्यूरेंसी खनन
- 20.2.4. पिरामिड योजनाएँ
- 20.2.5. अन्य संभावित अपराध और समस्याएँ

20.3. डीपफेक
- 20.3.2. मीडिया का प्रभाव
- 20.3.3. समाज के लिए खतरा
- 20.3.4. जांच तंत्र

20.4. कृत्रिम बुद्धिमत्ता का भविष्य
- 20.4.1. कृत्रिम बुद्धिमत्ता और संज्ञानात्मक कंप्यूटिंग
- 20.4.2. ग्राहक सेवा को सरल बनाने के लिए उपयोग

20.5. डिजिटल गोपनीयता
- 20.5.1. नेटवर्क में डेटा का मूल्य
- 20.5.2. नेटवर्क में डेटा का उपयोग
- 20.5.3. गोपनीयता और डिजिटल पहचान का प्रबंधन

20.6. साइबर संघर्ष, साइबर अपराधी और साइबर हमले
- 20.6.1. अंतर्राष्ट्रीय संघर्षों में साइबर सुरक्षा का प्रभाव
- 20.6.2. सामान्य जनसंख्या पर साइबर हमलों के परिणाम
- 20.6.3. साइबर अपराधियों के प्रकार सुरक्षा उपाय

20.7. टेलीवर्क
- 20.7.1. कोविड19 के दौरान और उसके बाद टेलीवर्क क्रांति
- 20.7.2. पहुँच बाधाएँ
- 20.7.3. हमलावर सतह की विविधता
- 20.7.4. कर्मचारी की जरूरतें

20.8. उभरती वायरलेस तकनीकें
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. मिलीमीटर तरंगें
- 20.8.4. "अधिक प्राप्त करें" के बजाय "स्मार्ट बनें" की प्रवृत्ति

20.9. नेटवर्क में भविष्य का संबोधन
- 20.9.1. आईपी एड्रेसिंग के साथ वर्तमान समस्याएँ
- 20.9.2. IPv6
- 20.9.2. IPv4+
- 20.9.3. IPv4 की तुलना में Ipv4+ के लाभ
- 20.9.4. IPv4 की तुलना में Ipv6 के लाभ

20.10. जनसंख्या में प्रारंभिक और सतत शिक्षा के बारे में जागरूकता बढ़ाने की चुनौती
- 20.10.1. सरकार की वर्तमान रणनीतियाँ
- 20.10.2. सीखने के प्रति जनसंख्या का प्रतिरोध
- 20.10.3. कंपनियों द्वारा अपनाई जाने वाली प्रशिक्षण योजनाएँ

> दोबारा मत सोचो, आप जानते हैं कि इस उच्च स्नातकोत्तर उपाधि के साथ, आप बहुत आगे तक जाएंगे”

05

प्रणाली

यह प्रशिक्षण कार्यक्रम सीखने का एक अलग तरीका प्रदान करता है। हमारी कार्यप्रणाली एक चक्रीय सीखने के तरीके के माध्यम से विकसित की गई है: **रीलर्निंग।**

उदाहरण के लिए, इस शिक्षण प्रणाली का उपयोग दुनिया के सबसे प्रतिष्ठित मेडिकल स्कूलों में किया जाता है और इसे न्यू इंग्लैंड जर्नल ऑफ़ मेडिसिन जैसे अत्यधिक प्रासंगिक प्रकाशनों द्वारा सबसे प्रभावी माना जाता है।

रीलर्निंग को जानें, एक प्रणाली जो आपको पारंपरिक रैखिक शिक्षा को छोड़ कर चक्रीय शिक्षण प्रणाली के माध्यम से आगे बढ़ती है: सीखने का एक तरीका जो अत्यधिक प्रभावी साबित हुआ है, विशेष रूप से उन विषयों में जिन्हें याद करने की आवश्यकता होती है"

सभी सामग्री को प्रासंगिक बनाने के लिए केस स्टडी

हमारा कार्यक्रम कौशल और ज्ञान विकसित करने का एक क्रांतिकारी तरीका प्रदान करता है। हमारा लक्ष्य बदलते, प्रतिस्पर्धी और अत्यधिक मांग वाले संदर्भ में कौशल को मजबूत करना है।

> टेक के साथ आप सीखने के ऐसे तरीके का अनुभव करने में सक्षम होंगे जो दुनिया भर के पारंपरिक विश्वविद्यालयों की नींव हिला रहा है"

आप पूरे पाठ्यक्रम में एक स्वाभाविक और प्रगतिशील शिक्षण के साथ, दोहराव पर आधारित एक सीखने की प्रणाली तक पहुँच प्राप्त करेंगे।

छात्र सहयोगी गतिविधियों और वास्तविक मामलों, वास्तविक व्यावसायिक वातावरण में जटिल परिस्थितियों का समाधान के माध्यम से सीखेंगे।

एक अभिनव और अलग शिक्षण पद्धति

यह TECH कार्यक्रम एक गहन शिक्षा है, जिसे बिल्कुल शुरुआत से बनाया गया है, जो इस क्षेत्र में राष्ट्रीय या अंतरराष्ट्रीय स्तर पर सबसे अधिक मांग वाली चुनौतियों और निर्णयों को प्रस्तुत करता है। इस पद्धति के माध्यम से, सफलता प्राप्त करने के लिए एक निर्णायक कदम उठाते हुए, व्यक्तिगत और व्यावसायिक विकास को बढ़ावा दिया जाता है। केस पद्धति, एक तकनीक जो इस सामग्री की नींव रखती है, गारंटी देती है कि सबसे वर्तमान आर्थिक, सामाजिक और व्यावसायिक वास्तविकता का पालन किया जाता है।

> हमारा कार्यक्रम आपको अनिश्चित वातावरण में नई चुनौतियों का सामना करने और अपने करियर में सफलता प्राप्त करने के लिए तैयार करता है"

केस पद्धति दुनिया के सर्वश्रेष्ठ सूचना प्रौद्योगिकी स्कूलों द्वारा अस्तित्व में आने के बाद से सबसे अधिक उपयोग की जाने वाली शिक्षण प्रणाली रही है। 1912 में विकसित की गयी केस पद्धति में छात्रों को वास्तविक जटिल स्थितियों के साथ प्रस्तुत करना शामिल था ताकि कानून के छात्र न केवल सैद्धांतिक सामग्री के आधार पर कानूनों को सीखें, बल्कि वे निर्णय ले सकें और उन्हें हल करने के तरीके पर आदर्श निर्णय ले सकें। 1924 में इसे हार्वर्ड में शिक्षण की मानक पद्धति के रूप में स्थापित किया गया।

एक निश्चित स्थिति में, एक पेशेवर को क्या करना चाहिए? यह वह प्रश्न है जिसका सामना हम केस मेथड में करते हैं, एक कार्य उन्मुख सीखने की पद्धति। कार्यक्रम के दौरान, छात्रों को कई वास्तविक मामलों का सामना करेंगे। उन्हें अपने सभी ज्ञान को एकीकृत करना , जांच करनी होगा, बहस करनी होगा और अपने विचारों और निर्णयों का बचाव करना होगा।

रीलर्निंग प्रणाली

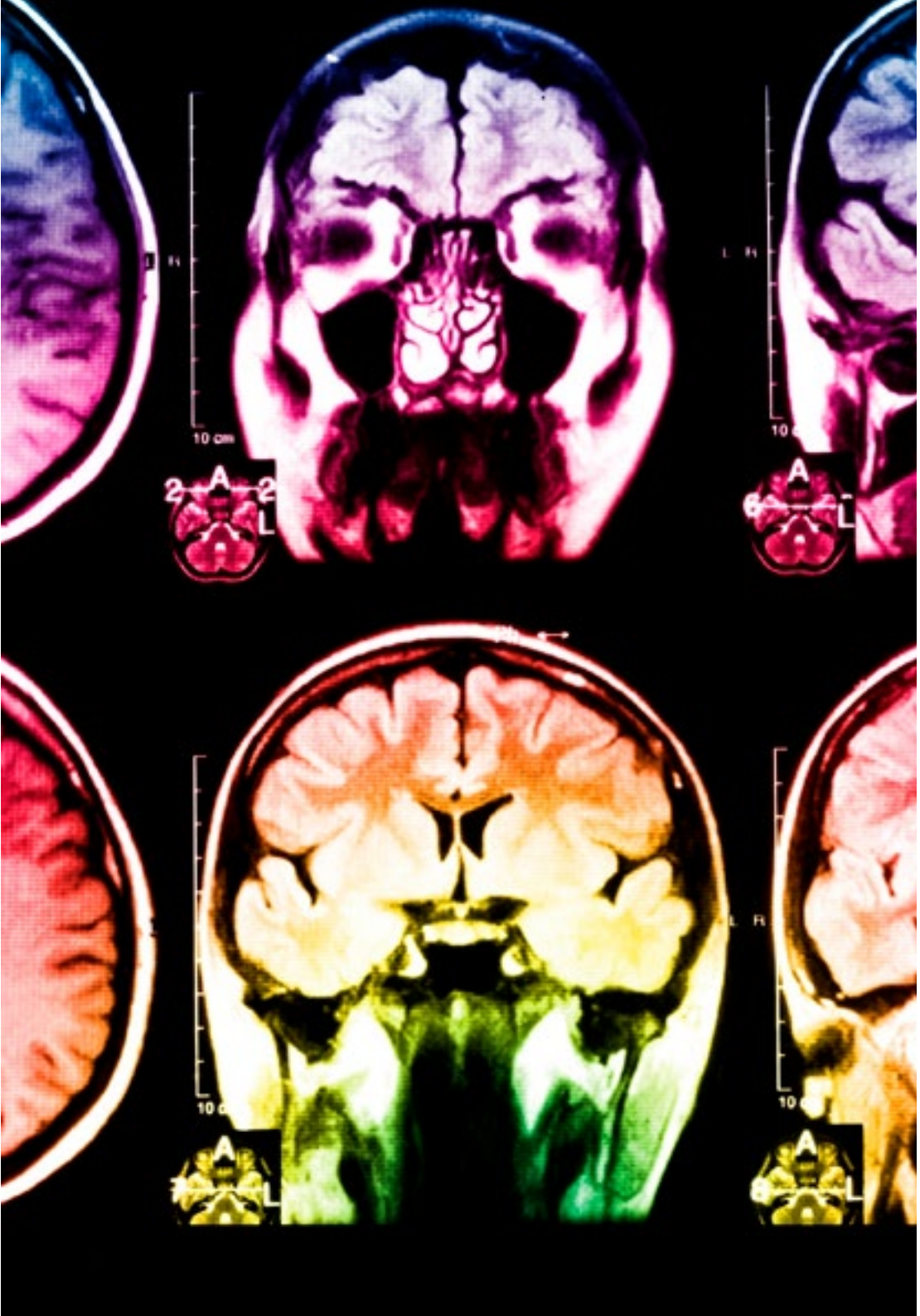
TECH प्रभावी रूप से दोहराव पर आधारित 100% ऑनलाइन शिक्षण प्रणाली के साथ केस स्टडी पद्धति को जोड़ती है, जो प्रत्येक पाठ में अलग-अलग शिक्षात्मक तत्वों को जोड़ती है।

हम 100% ऑनलाइन शिक्षण पद्धति के साथ एक सर्वश्रेष्ठ केस स्टडी को बढ़ावा देते हैं: री लर्निंग।

> 2019 में हमने दुनिया के सभी ऑनलाइन स्पेनिश विश्वविद्यालयों में सीखने के सर्वोत्तम परिणाम प्राप्त किए।

TECH में आप भविष्य के प्रबंधकों को प्रशिक्षित करने के लिए डिज़ाइन की गई एक अग्रग्रामी पद्धति से सीखेंगे। विश्व शिक्षाशास्त्र में सबसे आगे इस पद्धति को रीलर्निंग कहा जाता है।

हमारा विश्वविद्यालय इस सफल पद्धति का उपयोग करने के लिए लाइसेंस प्राप्त एकमात्र स्पेनिश-भाषी विश्वविद्यालय है। 2019 में, हम स्पेनी भाषा में सर्वश्रेष्ठ ऑनलाइन विश्वविद्यालय के संकेतकों के संबंध में अपने छात्रों के समग्र संतुष्टि स्तर (शिक्षण गुणवत्ता, सामग्री की गुणवत्ता, पाठ्यक्रम संरचना, उद्देश्यों...) में सुधार करने में कामयाब रहे।



हमारे कार्यक्रम में, सीखना एक रैखिक प्रक्रिया नहीं है, लेकिन यह एक सर्पिल (सीखना, भूलना, भूलना और फिर से सीखना) प्रक्रिया में होता है। इसलिए, इनमें से प्रत्येक तत्व को सकेन्द्री रूप से संयोजित किया जाता है। इस पद्धति के साथ 650,000 से अधिक विश्वविद्यालय के स्नातकों को जैव रसायन, आनुवंशिकी, सर्जरी, अंतरराष्ट्रीय कानून, प्रबंधन कौशल, खेल विज्ञान, दर्शन, कानून, इंजीनियरिंग, पत्रकारिता, इतिहास या बाजार और वित्तीय साधनों जैसे विविध क्षेत्रों में अभूतपूर्व सफलता के साथ प्रशिक्षित किया गया है। यह सब अत्यधिक मांग वाले माहौल में, उच्च सामाजिक आर्थिक प्रोफ़ाइल वाले विश्वविद्यालय के छात्रों और 43.5 वर्ष की औसत आयु के साथ।

> रीलर्निंग आपको कम प्रयास और अधिक प्रदर्शन के साथ सीखने, अपने प्रशिक्षण में अधिक शामिल होने, एक महत्वपूर्ण भावना विकसित करने, बचाव तर्क और विपरीत राय रखने में मदद करेगा: सफलता के लिए एक सीधा समीकरण।

न्यूरोसाइंस के क्षेत्र में नवीनतम वैज्ञानिक प्रमाणों के आधार पर, हम न केवल सूचनाओं, विचारों, छवियों और यादों को व्यवस्थित करना जानते हैं, बल्कि हम यह भी जानते हैं कि जिस स्थान और संदर्भ में हमने कुछ सीखा है, वह हमारे लिए याद रखने में सक्षम होने के लिए आवश्यक है। इसे हिप्पोकैम्पस में संग्रहीत करें, ताकि इसे हमारी दीर्घकालिक स्मृति में बनाए रखा जा सके।

इस तरह, और जिसे न्यूरोकॉग्निटिव संदर्भ-निर्भर ई-लर्निंग कहा जाता है, हमारे कार्यक्रम के विभिन्न तत्व उस संदर्भ से जुड़े होते हैं जहां प्रतिभागी अपने पेशेवर अभ्यास को विकसित करता है।

यह कार्यक्रम पेशेवरों के लिए सावधानीपूर्वक तैयार की गई सर्वोत्तम शैक्षिक सामग्री प्रदान करता है:

अध्ययन सामग्री

सभी शिक्षण सामग्री उन विशेषज्ञों द्वारा बनाई गई हैं जो पाठ्यक्रम को पढ़ाने जा रहे हैं, विशेष रूप से उनके लिए, ताकि शैक्षिक विकास वास्तव में विशिष्ट और ठोस हो।

TECH की ऑनलाइन कार्य पद्धति बनाने के लिए इन सामग्रियों को तब दृश्य-श्रव्य प्रारूप में लागू किया जाता है। यह सब, सबसे नवीन तकनीकों के साथ जो छात्र को उपलब्ध कराई गई प्रत्येक सामग्री में उच्च गुणवत्ता वाली सामग्री प्रदान करते हैं।

मास्टर क्लास

तीसरे-पक्ष विशेषज्ञ अवलोकन की उपयोगिता पर वैज्ञानिक प्रमाण हैं।

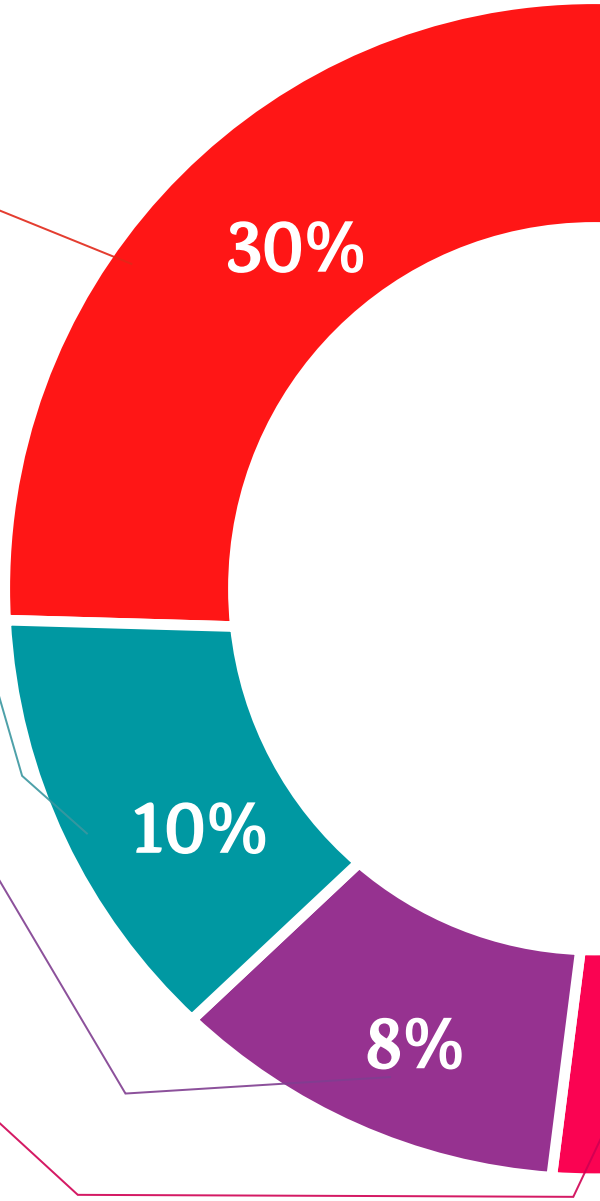
तथाकथित लर्निंग फ्रॉम एक्सपर्ट ज्ञान और स्मृति को पुष्ट करता है, और भविष्य के कठिन निर्णयों में विश्वास पैदा करता है।

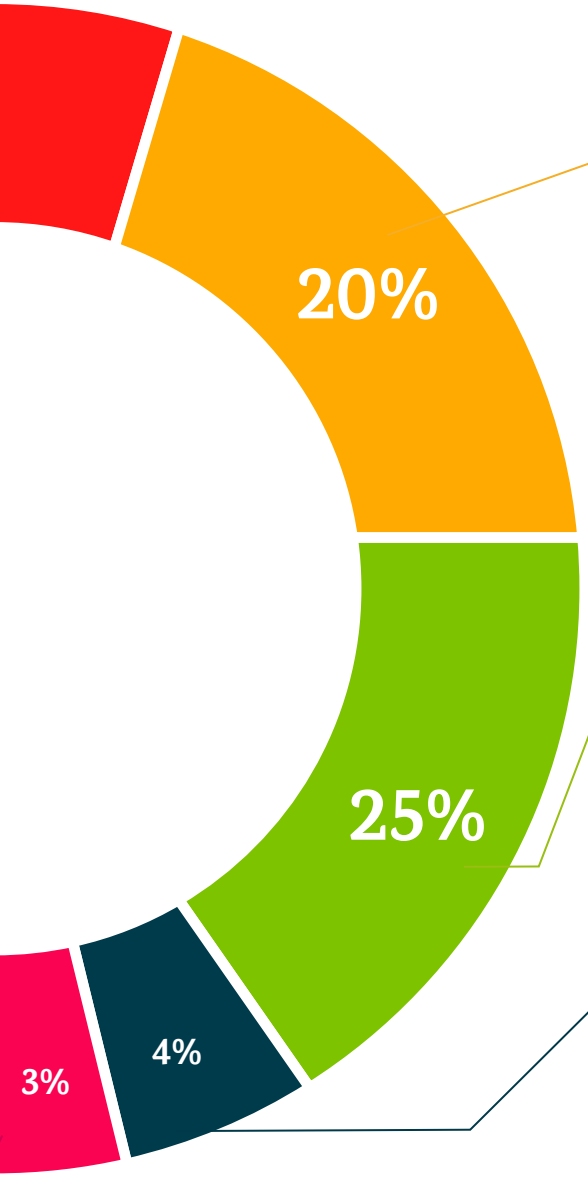
कौशल और दक्षता अभ्यास

वे प्रत्येक विषयगत क्षेत्र में विशिष्ट कौशल और क्षमताओं को विकसित करने के लिए गतिविधियाँ करेंगे। हम जिस वैश्वीकरण में रहते हैं, उसके ढांचे के भीतर एक विशेषज्ञ को विकसित करने के लिए आवश्यक कौशल और क्षमताओं को प्राप्त करने और विकसित करने के लिए अभ्यास और गतिशीलता।

अग्रिम पठन

हाल के लेख, आम सहमति दस्तावेज़ और अंतर्राष्ट्रीय दिशानिर्देश, और अन्य। टेक वर्चुअल लाइब्रेरी में, छात्रों को अपना प्रशिक्षण पूरा करने के लिए आवश्यक सभी चीजों तक पहुंच प्राप्त होगी।





केस स्टडी

वे इस स्थिति के लिए स्पष्ट रूप से चुने गए सर्वोत्तम केस स्टडी का चयन पूरा करेंगे। अंतर्राष्ट्रीय परिदृश्य पर सर्वश्रेष्ठ विशेषज्ञों द्वारा प्रस्तुत, विश्लेषण और पर्यवेक्षण के मामले।

इंटरैक्टिव सारांश

टेक टीम सामग्री को मल्टीमीडिया टुकड़ों में आकर्षक और गतिशील तरीके से प्रस्तुत करती है जिसमें ज्ञान को समेकित करने के लिए ऑडियो, वीडियो, छवियां, आरेख और अवधारणा मानचित्र शामिल होते हैं।

मल्टीमीडिया सामग्री की प्रस्तुति के लिए इस विशेष शैक्षिक प्रणाली को माइक्रोसॉफ्ट द्वारा "यूरोप में सफलता की कहानी" के रूप में सम्मानित किया गया था।

परीक्षण और पुनर्परीक्षण

छात्र के ज्ञान का मूल्यांकन और आत्म-मूल्यांकन गतिविधियों और अभ्यासों के माध्यम से पूरे कार्यक्रम में समय-समय पर मूल्यांकन और पुनर्मूल्यांकन किया जाता है ताकि छात्र यह सत्यापित कर सके कि वह अपने लक्ष्यों को कैसे प्राप्त कर रहा है।

07

उपाधि

सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधि में उच्च स्नातकोत्तर उपाधि, सबसे परिशुद्ध और अद्यतित प्रशिक्षण के अलावा, TECH Global University द्वारा जारी स्नातकोत्तर उपाधि में प्रवेश की गारंटी देता है।

इस कार्यक्रम को सफलतापूर्वक पूरा करें और यात्रा या श्रमसाध्य कागजी कार्रवाई के बिना अपनी विश्वविद्यालय की उपाधि प्राप्त करें”

यह निजी योग्यत कार्यक्रम आपको दुनिया के सबसे बड़े ऑनलाइन विश्वविद्यालय, TECH Global University द्वारा समर्थित **सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधि में उच्च स्नातकोत्तर उपाधि** डिप्लोमा प्राप्त करने की अनुमति देगा।

TECH Global University एक आधिकारिक यूरोपीय विश्वविद्यालय है जिसे अंडोरा सरकार (आधिकारिक बुलेटिन) द्वारा सार्वजनिक रूप से मान्यता प्राप्त है। अंडोरा 2003 से यूरोपीय उच्च शिक्षा क्षेत्र (ईएचईए) का हिस्सा है। ईएचईए यूरोपीय संघ द्वारा प्रवर्तित एक पहल है जिसका उद्देश्य अंतरराष्ट्रीय प्रशिक्षण ढांचे को व्यवस्थित करना और इस क्षेत्र के सदस्य देशों की उच्च शिक्षा प्रणालियों में सामंजस्य स्थापित करना है। यह परियोजना छात्रों, शोधकर्ताओं और शिक्षाविदों के बीच सहयोग और गतिशीलता बढ़ाने के लिए सामान्य मूल्यों, सहयोगी उपकरणों के कार्यान्वयन और इसके गुणवत्ता आश्वासन तंत्र को मजबूत करने को बढ़ावा देती है।

यह TECH Global University निजी योग्यता सतत शिक्षा और पेशेवर अद्यतनीकरण का एक यूरोपीय कार्यक्रम है जो ज्ञान के अपने क्षेत्र में दक्षताओं के अधिग्रहण की गारंटी देता है, जो कार्यक्रम पूरा करने वाले छात्र को उच्च पाठ्यचर्या मूल्य प्रदान करता है।

उपाधि: **सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधि में उच्च स्नातकोत्तर उपाधि**

रुपात्मकता: **ऑनलाइन**

अवधि: **2 वर्ष**

प्रमाणन: **120 ECTS**

tech global university

श्री/श्रीमती _____, पहचान-पत्र संख्या _____,

को पाठ्यक्रमों को सफलतापूर्वक पूरा करने पर और क्रेडिट प्राप्त करने पर

सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधि में उच्च स्नातकोत्तर उपाधि

यह 3,600 घंटे का एक निजी योग्यता कार्यक्रम है, जिसकी अवधि 60 ईसीटीएस के बराबर है, जिसकी आरंभ तिथि dd/mm/yyyy और समाप्ति तिथि dd/mm/yyyy है।

TECH Global University एक विश्वविद्यालय है जिसे आधिकारिक तौर पर 31 जनवरी 2024 को अंडोरा सरकार द्वारा मान्यता प्राप्त है, जो यूरोपीय उच्च शिक्षा क्षेत्र (ईएचईए) से संबंधित है।

28 फरवरी 2024 को, अंडोरा ला वेला में

डॉ. Pedro Navarro Illana
रेक्टर

विशिष्ट TECH कोड: AFWOR23S techtitute.com/certificates

सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधि में उच्च स्नातकोत्तर उपाधि

पाठ्यचर्या

पाठ्यक्रम	विषय	ECTS	तरीका	पाठ्यक्रम	विषय	ECTS	तरीका
1°	एक व्यावसायिक संस्था में डेटा विश्लेषिकी	6	OB	2°	साइबरइंटेलिजेंस और साइबर सुरक्षा	6	OB
1°	डेटा प्रबंधन, डेटा हेरफेर और डेटा साइंस रिपोर्टिंग	6	OB	2°	मेज़बान सुरक्षा	6	OB
1°	डेटा साइंस की नींव के रूप में IoT उपकरणों और प्लेटफ़ॉर्म	6	OB	2°	नेटवर्क सुरक्षा (परिधि)	6	OB
1°	डेटा विश्लेषण के लिए ग्राफिकल प्रतिनिधित्व	6	OB	2°	स्मार्टफ़ोन सुरक्षा	6	OB
1°	साइंस डेटा उपकरण	6	OB	2°	आईओटी सुरक्षा	6	OB
1°	डेटा माइनिंग चयन, प्रसंस्करण और परिवर्तन	6	OB	2°	नैतिक हैकिंग	6	OB
1°	संभाव्यता सिद्धांत का पूर्वानुमान और विश्लेषण	6	OB	2°	रिवर्स इंजीनियरिंग	6	OB
1°	इंटेलिजेंट प्रणाली का डिजाइन और विकास	6	OB	2°	सुरक्षित विकास	6	OB
1°	डेटा-सघन प्रणाली और वास्तुकला	6	OB	2°	फॉरेंसिक विश्लेषण	6	OB
1°	व्यावहारिक अनुप्रयोगव्यावसायिक क्षेत्रों में डेटा साइंस	6	OB	2°	IT सुरक्षा में वर्तमान और भविष्य की चुनौतियाँ	6	OB

डॉ. Pedro Navarro Illana
रेक्टर

tech global university

*अपॉस्टिल कन्वेन्शन। यदि छात्र अपॉस्टिल कन्वेन्शन की कागजी डिग्री का अनुरोध करता है, तो TECH Global University अतिरिक्त कीमत पर इसकी प्राप्ति के लिए उचित कदम उठाएगा।

tech global university

उच्च स्नातकोत्तर उपाधि

सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधि

- रुपात्मकता: ऑनलाइन
- अवधि: 2 वर्ष
- उपाधि: TECH Global University
- प्रमाणन: 120 ECTS
- अनुसूची: अपनी गति से
- परीक्षा: ऑनलाइन

उच्च स्नातकोत्तर उपाधि

सुरक्षित सूचना प्रबंधन में उच्च स्नातकोत्तर उपाधिन

tech global university