# ماجستير متقدم

# إدارة المعلومات الآمنة

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

# ماجستير متقدم

## إدارة المعلومات الآمنة

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **سنتين**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- عدد الساعات المخصصة للدراسة: **16 ساعات أسبوعيًا**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

رابط الدخول إلى الموقع الإلكتروني: **www.techtitute.com/ae/information-technology/advanced-master-degree/advanced-master-degree-secure-information-management**

# الفهرس


# 01
# المقدمة

تهيمن البيئة الرقمية على العالم بشكل يومي. والعالم الرقمي يدير عددًا كبيرًا من الأنشطة من مختلف المجالات. وبالتالي لم يعد من الممكن فهم أوقات الفراغ أو العمل أو الاتصال بالأصدقاء والعائلة بدون الإنترنت وجميع الأدوات الموجودة على الإنترنت. لهذا السبب يتم نقل كميات هائلة من المعلومات يوميًا من البيانات غير الضارة في المحادثات عبر الشبكات الاجتماعية وتطبيقات المراسلة إلى المعلومات الحساسة للغاية ذات الطبيعة الشخصية والمهنية المستضافة على مواقع الويب المصرفية أو التجارية. في هذه البانوراما المعقدة هناك حاجة إلى متخصصين يمكنهم إدارة جميع أنواع المعلومات التي تنتمي إلى هذه المناطق مع إيلاء الاهتمام الكافي لأمانِها. تبحث العديد من الشركات عن موظفين بهذا الملف الشخصي لحماية معلوماتها.

يحاول بعض الأشخاص ذوي الأهداف السيئة كل يوم تعريض أمن الشركات والمؤسسات التي تدير بيانات قيّمة للغاية للخطر بشكل دائم: يمكنك أن تكون الحامي الأكبر لتلك المعلومات"

كل يوم يقوم ملايين الأشخاص بجميع أنواع الأنشطة على الإنترنت. يقومون بمراجعة الأخبار والتحدث مع الأصدقاء والعائلة وتبادل الآراء على الشبكات الاجتماعية وتنفيذ المهام الإدارية في الشركات والمؤسسات المختلفة ومشاركة جميع أنواع الملفات أو القيام بمهام متعلقة بالعمل. وبالتالي يتم إنشاء ونقل كميات لا حصر لها من البيانات في كل لحظة في جميع أنحاء العالم.

إن إدارتها بأمان مناسب ليست مهمة سهلة لأنها تتطلب سلسلة من المعرفة المحددة من مختلف المجالات التي لن يكونوا على اتصال بها عادة. لهذا السبب يعد هذا الماجستير المتقدم في إدارة المعلومات الآمنة فرصة رائعة للغاية لجميع المهندسين ومحترفي تكنولوجيا المعلومات الذين يرغبون في دمج إدارة المعلومات والأمن السيبراني ليصبحوا أعظم المتخصصين في كلا المجالين.

تتعامل العديد من الشركات والمؤسسات مع بيانات حساسة للغاية وقيمة تتطلب الإدارة السليمة والحفظ والمراقبة. لا يزال هناك عدد قليل من الخبراء في كلا المجالين الذين يمكنهم الاعتناء بإدارتها الصحيحة. وبالتالي سيكون الطلاب الذين أكملوا هذه الدرجة في أفضل وضع للوصول إلى المناصب العليا في الشركات التي تسعى إلى تأمين معلوماتهم الرقمية.

للقيام بذلك صممت TECH أفضل محتوى وجمعت بين أفضل المعلمين الذين يتمتعون بخبرة مهنية واسعة في هذه المجالات بحيث يتلقى الطلاب التعليم الأكثر شمولاً ممكنًا ويمكنهم التقدم في مكان العمل.

تحتوي درجة **الماجستير المتقدم في إدارة المعلومات الآمنة** على البرنامج العلمي الأكثر اكتمالا وحداثة في السوق. ومن أبرز ميزاته:

- تطوير الحالات العملية التي يقدمها خبراء في نظم المعلومات
- محتوياتها الرسومية والتخطيطية والعملية البارزة التي يتم تصورها تجمع المعلومات العلمية للممارسة الصحية حول تلك التخصصات الأساسية للممارسة المهنية
- التدريبات العملية حيث يتم إجراء عملية التقييم الذاتي لتحسين التعليم
- تركيزها الخاص على المنهجيات المبتكرة في إدارة وأمن البيانات الرقمية
- دروس نظرية وأسئلة للخبراء ومنتديات مناقشة حول القضايا الخلافية وأعمال التفكير الفردي
- توفر الوصول إلى المحتوى من أي جهاز ثابت أو محمول متصل إلى الإنترنت

> يتم تسجيل كل ما نقوم به في العالم الرقمي. اجعل الإنترنت مكانًا أكثر أمانًا بفضل هذا الماجستير المتقدم"

أفضل الشركات في الدولة سيثقون بك في إدارة وأمن بياناتهم
عند الانتهاء من دراسة هذا البرنامج"

يجمع هذا الماجستير المتقدم بين تخصصين أساسيين
لمستقبل حياتك المهنية. سجل الآن وحقق كل أهدافك.

تعرف على كل شيء عن أمن البيانات وإدارتها وشاهد
كيف تتقدم مهنيًا في وقت قصير جدًا

وهي تضم في هيئة التدريس مهنيين ينتمون إلى مجال الحوسبة والذين يتدفقون في هذا البرنامج على خبرة عملهم فضلاً عن المتخصصين المعترف بهم من المجتمعات الرائدة والجامعات المرموقة.

بفضل محتوى الوسائط المتعددة المُعد بأحدث التقنيات التعليمية إلى التعلم المهني والسياقي أي في بيئة محاكاة التي ستوفرها هذه الشهادة الجامعية من تدريب ضمن مواقف حقيقية.

يركز تصميم هذا البرنامج على التعلم القائم على المشكلات، والذي يجب على الطالب من خلاله محاولة حل الحالات المختلفة للممارسة المهنية التي تُطرَح على مدار هذه البرنامج الأكاديمية. للقيام بذلك سيحصل على مساعدة من نظام جديد من مقاطع الفيديو التفاعلية التي أعدها خبراء معترف بهم.

02

# الأهداف

الهدف الرئيسي من هذا الماجستير المتقدم في إدارة المعلومات الآمنة هو تزويد طلابها بأفضل المعارف في فرعين مختلفين ولكن مترابطين للحوسبة والهندسة: إدارة البيانات في البيئة الرقمية والأمن السيبراني. من خلال الجمع بين هذين المجالين سيتمكن علماء الكمبيوتر والمهنيون الذين يأخذون هذا البرنامج من تطبيق أفضل الحلول في كل موقف ينشأ في حياتهم المهنية مما يوفر لشركاتهم الأدوات الأكثر ملاءمة لإدارة وحماية جميع أنواع المعلومات الحساسة.

هدفك هو أن تكون أفضل متخصص في شركتك و *TECH* تقدم لك الأدوات اللازمة لتحقيق ذلك"



## الأهداف العامة

- تحليل فوائد تطبيق تقنيات تحليل البيانات في كل قسم من أقسام المؤسسة التجارية
- تطوير أسس معرفة احتياجات وتطبيقات كل قسم
- توليد المعرفة المتخصصة لاختيار الأداة الصحيحة
- اقتراح التقنيات والأهداف لتكون منتجة قدر الإمكان وفقًا للقسم
- تحليل دور محلل الأمن السيبراني
- التعمق في الهندسة الاجتماعية وطرقها
- فحص منهجيات OSINT، HUMINT، OWASP، PTEC، OSSTM، OWISAM
- إجراء تحليل للمخاطر وتعلم مقاييس المخاطر
- تحديد الاستخدام المناسب لإخفاء الهوية واستخدام الشبكات مثل TOR و I2P و Freenet
- تجميع اللوائح الحالية المتعلقة بالأمن السيبراني
- توليد المعرفة المتخصصة لأداء تدقيق الأمن
- تطوير سياسات الاستخدام المناسبة
- فحص أنظمة الكشف والوقاية لأهم التهديدات
- تقييم أنظمة الكشف عن التهديدات الجديدة بالإضافة إلى تطورها فيما يتعلق بالحلول الأكثر تقليدية
- تحليل منصات المحمول الرئيسية الحالية وخصائصها واستخداماتها
- تحديد وتحليل وتقييم المخاطر الأمنية لأجزاء مشروع الإنترنت IoT
- تقييم المعلومات التي تم الحصول عليها وتطوير آليات الوقاية والاختراق
- تطبيق الهندسة العكسية على بيئة الأمن السيبراني
- تحديد الاختبارات التي يجب إجراؤها على البرنامج المطور
- جمع كل الأدلة والبيانات الموجودة لتنفيذ تقرير المعلومات الشرعية
- تقديم تقرير المعلومات الشرعية بشكل صحيح
- تحليل الحالة الحالية والمستقبلية لأمن الكمبيوتر
- فحص مخاطر التقنيات الناشئة الجديدة
- تجميع التقنيات المختلفة فيما يتعلق بأمن الكمبيوتر

## الأهداف المحددة

### الوحدة 1. تحليلات البيانات في المؤسسة التجارية

- تطوير المهارات التحليلية لاتخاذ قرارات الجودة
- إختبار الحملات التسويقية والتواصلية الفعالة
- تحديد إنشاء وثائق التقييم ومؤشرات الأداء الرئيسية حسب القسم
- توليد المعرفة المتخصصة لتطوير التحليل التنبئي
- اقتراح خطط الأعمال والولاء بناءً على أبحاث السوق
- تنمية القدرة على الاستماع إلى العميل
- تطبيق المعرفة الإحصائية والكمية والفنية في مواقف حقيقية

### الوحدة 2. إدارة ومعالجة البيانات والمعلومات لعلوم البيانات

- القيام بإجراء تحليل للبيانات
- توحيد البيانات المتنوعة: تحقيق تناسق المعلومات
- إنتاج المعلومات ذات الصلة والفعالة لاتخاذ القرار
- تحديد أفضل الممارسات لإدارة البيانات حسب نوعها واستخداماتها
- إنشاء سياسات الوصول إلى البيانات وإعادة استخدامها
- ضمان الأمن والتوافر: توافر وسلامة وسرية المعلومات
- فحص أدوات إدارة البيانات من خلال لغات البرمجة

### الوحدة 3. أجهزة ومنصات IoT كأساس لعلوم البيانات

- تحديد ما هو IoT (إنترنت الأشياء) و IIoT (إنترنت الأشياء الصناعي)
- إختباراتحاد الإنترنت الصناعي
- تحليل ماهية هندسة العمارة المرجعية لإنترنت الأشياء IoT
- معالجة أجهزة استشعار وأجهزة إنترنت الأشياء IoT وتصنيفها
- تحديد بروتوكولات الاتصالات والتقنيات المستخدمة في إنترنت الأشياء IoT
- فحص الأنظمة الأساسية السحابية المختلفة في إنترنت الأشياء: الغرض العام، صناعي، مفتوح المصدر
- تطوير آليات تبادل البيانات
- تحديد المتطلبات والاستراتيجيات الأمنية
- التعريف بمجالات تطبيقات IoT و IIoT

### الوحدة 4. العرض البياني لتحليل البيانات

- توليد المعرفة المتخصصة في عرض البيانات والتحليلات
- إختبار الأنواع المختلفة من البيانات المجمعة
- إنشاء العروض البيانية الأكثر استخدامًا في مجالات مختلفة
- تحديد مبادئ التصميم في تصور البيانات
- تقديم السرد البياني كأداة
- تحليل أدوات البرمجيات المختلفة للرسم البياني وتحليل البيانات الاستكشافية

### الوحدة 5. أدوات علوم البيانات

- تطوير المهارات لتحويل البيانات إلى معلومات يمكن من خلالها استخلاص المعرفة
- تحديد الخصائص الرئيسية لمجموعة البيانات وهيكلها ومكوناتها وآثار توزيعها في النمذجة
- دعم اتخاذ القرار من خلال إجراء تحليلات كاملة سابقة للبيانات
- تطوير المهارات لحل الحالات العملية باستخدام تقنيات علوم البيانات
- إنشاء أنسب الأدوات والأساليب العامة لنمذجة كل مجموعة بيانات Dataset بناءً على المعالجة المسبقة التي تم إجراؤها
- تقييم النتائج بشكل تحليلي وفهم تأثير الاستراتيجية المختارة على المقاييس المختلفة
- إظهار القدرة الحاسمة قبل النتائج التي تم الحصول عليها بعد تطبيق طرق المعالجة المسبقة أو النمذجة

### الوحدة 6. استخراج البيانات. الاختيار والمعالجة والتحويل

- توليد معرفة متخصصة بالإحصاءات السابقة لأي تحليل وتقييم للبيانات
- تطوير المهارات اللازمة لتحديد وإعداد وتحويل البيانات
- تقييم المنهجيات المختلفة المقدمة وتحديد المزايا والعيوب
- إختيار المشكلات في بيئات البيانات عالية الأبعاد
- تطوير تنفيذ الخوارزميات المستخدمة في الإعداد المسبق لمعالجة البيانات
- إظهار القدرة على تفسير تصور البيانات للتحليل الوصفي
- تطوير المعرفة المتقدمة حول مختلف تقنيات إعداد البيانات الحالية لتنظيف البيانات وتطبيعها وتحويلها

### الوحدة 7. القدرة على التنبؤ وتحليل الظواهر العشوائية

- تحليل السلاسل الزمنية
- تطوير الصياغة والخصائص الأساسية لنماذج المتسلسلة الزمنية أحادية المتغير
- فحص منهجية النمذجة والتنبؤ بالسلاسل الزمنية الحقيقية
- تحديد النماذج أحادية المتغير بما في ذلك القيم المتطرفة
- تطبيق نماذج الانحدار الديناميكي وتطبيق المنهجية لبناء النماذج المذكورة من السلاسل المرصودة
- تناول التحليل الطيفي للسلاسل الزمنية أحادية المتغي وكذلك الجوانب الأساسية المتعلقة بالاستدلال بناءً على مخطط الرسم البياني وتفسيرها
- تقدير احتمالية واتجاه المتسلسلة الزمنية لأفق زمني معين

### الوحدة 8. تصميم وتطوير الأنظمة الذكية

- تحليل الانتقال من معلومات إلى معرفة
- تطوير أنواع مختلفة من تقنيات التعلم الآلي
- فحص المقاييس والنتائج لتحديد جودة النماذج
- تنفيذ خوارزميات التعلم الآلي المختلفة
- التعرف على نماذج التفكير الاحتمالية
- وضع أسس التعلم العميق
- إظهار المهارات المكتسبة لفهم خوارزميات التعلم الآلي المختلفة

### الوحدة 9. معماريات وأنظمة للاستخدام المكثف للبيانات

- تحديد متطلبات أنظمة البيانات الضخمة
- فحص نماذج البيانات المختلفة وتحليل قواعد البيانات
- تحليل الوظائف الرئيسية للأنظمة الموزعة وأهميتها في أنواع مختلفة من الأنظمة
- تقييم التطبيقات المستخدمة على نطاق واسع والتي تستخدم أساسيات الأنظمة الموزعة لتصميم أنظمتها
- تحليل كيفية تخزين قواعد البيانات واسترداد المعلومات
- تحديد نماذج النسخ المختلفة والمشكلات المرتبطة بها
- تطوير أشكال التقسيم والمعاملات الموزعة
- تحديد أنظمة الدُفعات وأنظمة الحوسبة في زمن حقيقي (تقريبا)

### الوحدة 10. التطبيق العملي لعلوم البيانات في قطاعات النشاط التجاري

- تحليل حالة فن الذكاء الاصطناعي (IA) وتحليلات البيانات
- تطوير المعرفة المتخصصة حول التقنيات الأكثر استخدامًا
- توليد فهم أفضل للتكنولوجيا من خلال حالات الاستخدام
- تحليل الاستراتيجيات المختارة لاختيار أفضل التقنيات لتنفيذها
- تحديد مجالات التطبيق
- فحص المخاطر الحقيقية والمحتملة للتكنولوجيا المطبقة
- اقتراح الفوائد المستمدة من الاستخدام
- تحديد الاتجاهات المستقبلية في قطاعات محددة

### الوحدة 11. الذكاء السيبراني والأمن السيبراني

- تطوير المنهجيات المستخدمة في الأمن السيبراني
- فحص دورة الذكاء وتأسيس تطبيقه في الذكاء السيبراني
- تحديد دور محلل المخابرات ومعوقات نشاط الإخلاء
- تحليل منهجيات OSINT، OWISAM، OSSTM، PTES، OWASP
- إنشاء الأدوات الأكثر شيوعًا لإنتاج المعلومات الاستخبارية
- إجراء تحليل للمخاطر ومعرفة المقاييس المستخدمة
- تحديد خيارات إخفاء الهوية واستخدام الشبكات مثل TOR و I2P و FreeNet
- تفصيل اللوائح الحالية بشأن الأمن السيبراني

### الوحدة 12. أمن المضيف

- تحديد سياسات النسخ الاحتياطي للبيانات الشخصية والمهنية
- تقييم الأدوات المختلفة لتقديم حلول لمشاكل أمنية محددة
- إنشاء آليات للحصول على نظام محدث
- فحص جهاز الكمبيوتر الخاص بك لاكتشاف الدخلاء
- تحديد قواعد الوصول إلى النظام
- فحص وتصنيف رسائل البريد الإلكتروني لتجنب الاحتيال
- إنشاء قوائم بالبرامج المسموح بها

### الوحدة 13. أمان الشبكة (المحيطية)

- تحليل هياكل الشبكة الحالية لتحديد المحيط الذي يجب علينا حمايته
- تطوير جدار حماية وتكوينات Linux محددة للتخفيف من الهجمات الأكثر شيوعًا
- قم بتجميع الحلول الأكثر استخدامًا مثل Snort و Suricata بالإضافة إلى تكوينها
- فحص الطبقات الإضافية المختلفة التي يوفرها الجيل التالي من جدران الحماية ووظائف الشبكة في بيئات السحابة
- تحديد أدوات حماية الشبكة واشرح سبب أهميتها للدفاع متعدد الطبقات

### الوحدة 14. أمان الهاتف الذكي

- فحص نواقل الهجوم المختلفة لتجنب أن تصبح هدفًا سهلاً
- تحديد الهجمات الرئيسية وأنواع البرامج الضارة التي يتعرض لها مستخدمو الأجهزة المحمولة
- تحليل أحدث الأجهزة لإنشاء أمان أكبر في التكوين
- تحديد الخطوات الرئيسية لإجراء اختبار الاختراق على كل من أنظمة iOS ومنصات Android
- تطوير المعرفة المتخصصة حول أدوات الحماية والأمن المختلفة
- إنشاء الممارسات الجيدة في البرمجة الموجهة للأجهزة المحمولة

### الوحدة 15. أمن إنترنت الأشياء IoT

- تحليل البنى الأساسية لإنترنت الأشياء IoT
- تصفح تقنيات الاتصال
- تطوير بروتوكولات التطبيق الأساسية
- تحديد الأنواع المختلفة للأجهزة الموجودة
- تقييم مستويات المخاطر ونقاط الضعف المعروفة
- تطوير سياسات الاستخدام الآمن
- تحديد شروط الاستخدام المناسبة لهذه الأجهزة

### الوحدة 16. القرصنة الأخلاقية

- تصفح أساليب IOSINT
- جمع المعلومات المتاحة في وسائل الإعلام العامة
- فحص الشبكات للحصول على معلومات الوضع النشط
- تطوير معامل الاختبار
- تحليل أدوات أداء Pentesting
- فهرسة وتقييم نقاط الضعف المختلفة للأنظمة
- تحديد المنهجيات المختلفة للقرصنة

### الوحدة 17. الهندسة العكسية

- تحليل مراحل المترجم
- تصفح بنية معالج x86 وبنية معالج ARM
- تحديد أنواع التحليل المختلفة
- وضع الحماية في بيئات مختلفة
- تطوير تقنيات تحليل البرامج الضارة المختلفة
- إنشاء الأدوات الموجهة لتحليل البرامج الضارة

### الوحدة 18. التنمية الآمنة

- تحديد المتطلبات اللازمة للتشغيل الصحيح للتطبيق بطريقة آمنة
- فحص ملفات السجل لفهم رسائل الخطأ
- تحليل الأحداث المختلفة وحدد ما يجب إظهاره للمستخدم وما يجب حفظه في السجلات
- إنشاء كود خالٍ من التعقيدات يمكن التحقق منه بسهولة
- تقييم الوثائق المناسبة لكل مرحلة من مراحل التطوير
- تحديد سلوك الخادم لتحسين النظام
- تطوير كود معياري وقابل لإعادة الاستخدام وقابل للصيانة

### الوحدة 19. التحليل الجنائي

- تحديد العناصر المختلفة التي تثبت الجريمة
- توليد المعرفة المتخصصة للحصول على البيانات من الوسائط المختلفة قبل ضياعها
- استعادة البيانات التي تم حذفها عمدًا
- تحليل السجلات وسجلات النظام
- تحديد كيفية تكرار البيانات حتى لا تغير الأصول
- اختبارات تحقق من أجل الاتساق
- إنشاء تقرير قوي وسلس
- تقديم الاستنتاجات بشكل متماسك
- تحديد كيفية الدفاع عن التقرير أمام السلطة المختصة
- تحديد استراتيجيات لجعل العمل عن بعد آمنًا

### الوحدة 20. التحديات الحالية والمستقبلية في أمن الكمبيوتر

- فحص استخدام العملات المشفرة وتأثيرها على الاقتصاد والأمن
- تحليل أوضاع المستخدمين ودرجة الأمية الرقمية
- تحديد نطاق استخدام *Blockchain*
- تقديم بدائل لـ IPv4 في عنونة الشبكة
- تطوير استراتيجيات لتدريب السكان على الاستخدام الصحيح للتقنيات
- توليد المعرفة المتخصصة لمواجهة التحديات الأمنية الجديدة ومنع سرقة الهوية
- تحديد استراتيجيات لجعل العمل عن بعد آمنًا

# 03
# الكفاءات

سيتمكن الطلاب الذين يُتِمون هذا الماجستير المتقدم في إدارة المعلومات الآمنة من أداء عدد كبير من المهام المتخصصة للغاية في مجالات إدارة البيانات والأمن السيبراني. وبالتالي يجمع هذا المؤهل بين الفرعين لتقديم معرفة تكميلية يمكن تجاوزها واستخدامها في مواقف وبيئات مهنية مختلفة. بهذه الطريقة سينفذ الطلاب عملية تعليمية شاملة ستوجههم ليكونوا متخصصين حقيقيين في هذا المجال.

ستجعلك المهارات الجديدة أعظم متخصص في مجالك المهني"

## الكفاءات العامة

- تطوير منظور فني وتجاري لتحليل البيانات
- فهم الخوارزميات والأنظمة الأساسية المختلفة ومعظم الأدوات الحالية لاستكشاف البيانات وتصورها وتنفيذها ومعالجتها وتحليلها
- تنفيذ رؤية عمل ضرورية لتعزيز القيمة كعنصر أساسي لاتخاذ القرار
- القدرة على معالجة مشاكل محددة في تحليل البيانات
- التعرف على المنهجيات المستخدمة في الأمن السيبراني
- تقييم كل نوع من أنواع التهديد لتقديم الحل الأمثل في كل حالة
- إنشاء حلول ذكية كاملة لأتمتة السلوك في حالة وقوع حوادث
- التعرف على كيفية تقييم المخاطر المرتبطة بنقاط الضعف خارج الشركة وداخلها
- التعرف على تطور وتأثير إنترنت الأشياء بمرور الوقت
- إثبات ضعف النظام ومهاجمته لأغراض وقائية وحل هذه المشكلات
- وضع الحماية *Sandboxing* في بيئات مختلفة
- التعرف على الإرشادات التي يجب على المطور الجيد اتباعها للامتثال للأمان اللازم

> هل تريد أن تتميز عن غيرك من المتخصصين ولكن لا تعرف كيف هي الطريقة؟ هذا الماجستير متقدم هو ما تبحث عنه"

## الكفاءات المحددة

- التخصص في علوم البيانات من منظور تقني وتجاري
- تصور البيانات بالطريقة الأنسب لتفضيل مشاركتها وفهمها بواسطة ملفات تعريف مختلفة
- تناول المجالات الوظيفية الأساسية للمؤسسة حيث يمكن لعلم البيانات تقديم أكبر قيمة
- تطوير دورة حياة البيانات وتصنيفها والتقنيات والمراحل اللازمة لإدارتها
- معالجة البيانات وتنفيذها باستخدام مكتبات ولغات محددة
- تطوير المعرفة المتقدمة في تقنيات التنقيب عن البيانات الأساسية لاختيار البيانات والمعالجة المسبقة والتحول
- تخصص في خوارزميات التعلم الآلي الرئيسية لاستخراج المعرفة المخفية من البيانات
- توليد المعرفة المتخصصة في المعمارية البرمجية وأنظمة البرمجيات اللازمة للاستخدام المكثف للبيانات
- تحديد كيف يمكن أن تكون إنترنت الأشياء IoT مصدرًا لتوليد البيانات والمعلومات الأساسية التي يمكن من خلالها تطبيق علم البيانات لاستخراج المعرفة
- تحليل الطرق المختلفة لتطبيق علم البيانات في قطاعات مختلفة أو رأسية من خلال التعلم من أمثلة حقيقية
- إجراء عمليات أمنية دفاعية
- امتلاك تصور عميق ومتخصص لأمن الكمبيوتر
- امتلاك معرفة متخصصة في مجال الأمن السيبراني والذكاء السيبراني
- امتلاك معرفة عميقة بالجوانب الأساسية مثل دورة الذكاء ومصادر الذكاء والهندسة الاجتماعية ومنهجية HUMINT، OSINT، وإخفاء الهوية وتحليل المخاطر والمنهجيات الحالية (OWASP، OWISAM، OSSTM، PTES) واللوائح الحالية بشأن الأمن السيبراني
- فهم أهمية ابتكار دفاع متعدد الطبقات يُعرف أيضًا باسم الدفاع في العمقوالذي يغطي جميع جوانب شبكة الشركة حيث يمكن أيضًا استخدام بعض المفاهيم والأنظمة التي سنراها وتطبيقها في بيئة محلية
- التعرف على كيفية تطبيق عمليات الأمان على الهواتف الذكية والأجهزة المحمولة
- تعرف على وسائل تنفيذ ما يسمى بالقرصنة الأخلاقية وحماية الشركة من هجوم إلكتروني
- التحقيق في حادثة الأمن السيبراني
- التعرف على تقنيات الهجوم والدفاع المختلفة الموجودة
- تحليل دور محلل الأمن السيبراني ومعرفة كيفية عمل الهندسة الاجتماعية وطرقها

04

# هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

يتم تدريس هذه الدرجة من قبل أفضل الأساتذة في مجالات الأمن السيبراني وإدارة البيانات الرقمية. تضمن خبرتهم حصول الطلاب على المحتوى الأكثر اكتمالاً وحداثة حتى يتمكنوا من تطبيقه مباشرة على حياتهم المهنية. وبهذه الطريقة، سينقل معلمو هذا الماجستير المتقدم في إدارة المعلومات الآمنة كل معارفهم إلى الطلاب مما يضمن أن يصبحوا متخصصين مؤهلين تأهيلاً عالياً حسب طلب الشركات الكبيرة في بلدانهم.

"يعلمك أفضل المتخصصين كيف تكون محترفًا رائدًا في هذا القطاع"

## المدير الدولي المُستضاف

الدكتور Frederic Lemieux مشهور دوليًا كخبير مبتكر وقائد ملهم في مجالات الاستخبارات والأمن القومي والأمن الداخلي والأمن السيبراني والتقنيات الإبتكارية. إن تفانيه المستمر ومساهماته ذات الصلة في البحث والتعليم تضعه كشخصية رئيسية في تعزيز سلامة وفهم التقنيات الناشئة اليوم. خلال حياته المهنية، وضع تصورات وأدار برامج أكاديمية متطورة في العديد من المؤسسات الشهيرة، مثل جامعة مونتريال وجامعة جورج واشنطن وجامعة جورج تاون.

خلال خلفيته الواسعة، نشر العديد من الكتب ذات الصلة للغاية، وكلها تتعلق بالاستخبارات الجنائية وعمل الشرطة والتهديدات الإلكترونية والأمن الدولي. كما ساهم بشكل كبير في مجال الأمن السيبراني من خلال نشر العديد من المقالات في المجلات الأكاديمية، التي تدرس السيطرة على الجريمة أثناء الكوارث الكبرى، ومكافحة الإرهاب، ووكالات الاستخبارات وتعاون الشرطة. وبالإضافة إلى ذلك، كان عضوا في حلقة النقاش ومتحدثا رئيسيا في مختلف المؤتمرات الوطنية والدولية، وعزز نفسه كمرجع في المجالين الأكاديمي والمهني.

قام الدكتور Lemieux بأدوار التحرير والتقييم في مختلف المنظمات الأكاديمية والخاصة والحكومية، مما يعكس تأثيره والتزامه بالتميز في مجال تخصصه. وبهذه الطريقة، قادته مسيرته الأكاديمية المرموقة إلى العمل كأستاذ للممارسات ومدير كلية لبرامج MPS في الذكاء التطبيقي وإدارة المخاطر في الأمن السيبراني وإدارة التكنولوجيا وإدارة تكنولوجيا المعلومات، في جامعة جورج تاون.

## د. Lemieux, Frederic

- باحث في مجال الاستخبارات والأمن السيبراني والتقنيات الابتكارية
- باحث في الاستخبارات والأمن السيبراني والتقنيات الابتكارية في جامعة جورج تاون
- مدير الماجستير في Information Technology Management بجامعة جورج تاون
- مدير الماجستير في Technology Management بجامعة جورج تاون
- مدير الماجستير في Cybersecurity Risk Management بجامعة جورج تاون
- مدير الماجستير في Applied Intelligence بجامعة جورج تاون
- أستاذ التدريب في بجامعة جورج تاون
- دكتوراه في علم الجريمة، كلية علم الجريمة، جامعة مونتريال
- بكالوريوس في علم الاجتماع، درجة ثانوية في علم النفس، من جامعة لافال
- عضو في New Program Roundtable Committee, من جامعة جورج تاون

بفضل *TECH* ستتمكن من التعلم مع أفضل المحترفين في العالم"

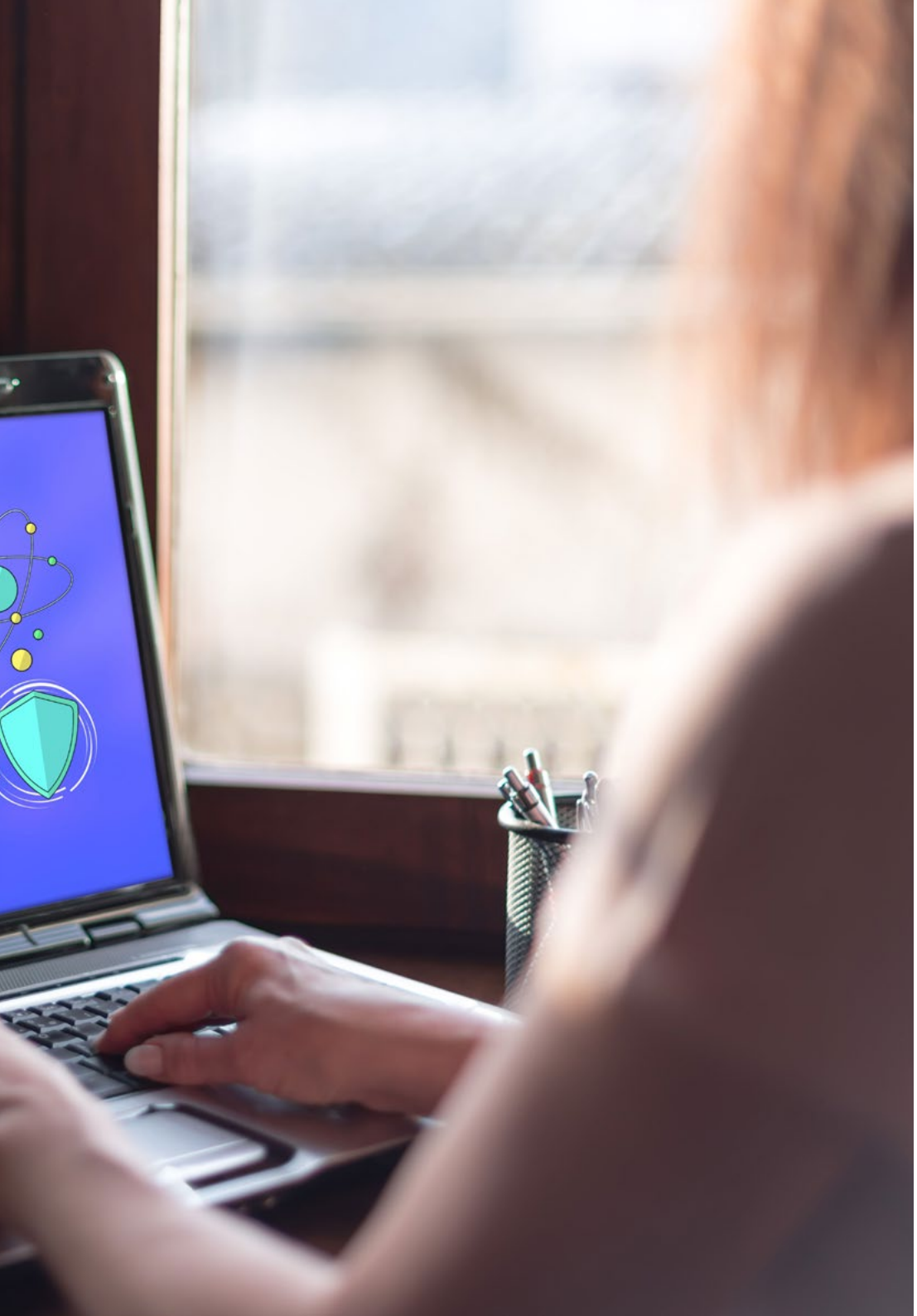
## هيكل الإدارة

### د. Peralta Martín-Palomino, Arturo

- الرئيس التنفيذي والمدير التقني في Prometeus Global Solutions
- مدير فني في Korporate Technologies في Korporate Technologies
- المدير التقني في AI Shepherds GmbH
- دكتوراه في هندسة الكمبيوتر من جامعة Castilla la Mancha
- دكتوراه في الاقتصاد والأعمال والتمويل من جامعة Camilo José Cela. جائزة الدكتوراه الاستثنائية
- دكتوراه في علم النفس من جامعة CastillaLa Mancha
- ماجستير في تكنولوجيا المعلومات المتقدمة من جامعة Castilla la Mancha
- MBA+E (ماجستير في إدارة الأعمال والهندسة التنظيمية) من جامعة Castilla la Mancha
- أستاذ مشارك، يدرس درجتي البكالوريوس والماجستير في هندسة الكمبيوتر، في جامعة Castilla la Mancha
- أستاذ ماجستير في البيانات الضخمة وعلوم البيانات بجامعة Valencia الدولية
- أستاذ ماجستير في الصناعة 4.0 وماجستير في التصميم الصناعي وتطوير المنتجات
- عضو في مجموعة أبحاث SMILe بجامعة Castilla la Mancha

**أ. Fernández Sapena, Sonia**

- مدرب أمن الكمبيوتر و القرصنة الأخلاقية. مركز خيتافي المرجعي الوطني في الحوسبة والاتصالات. مدريد
- مدرب معتمد من المجلس الإلكتروني. مدريد
- مدرب في الشهادات التالية: EXIN Ethical Hacking Foundation والمؤسسة الأمنية EXIN Cyber & IT. مدريد
- مدرب خبير معتمد من قبل CAM من الشهادات المهنية التالية: أمن الكمبيوتر (IFCT0190)، إدارة شبكات الصوت والبيانات (IFCM0310)، إدارة شبكات الإدارات (IFCT0410)، إدارة الإنذارات في شبكات الاتصالات (IFCM0410)، مشغل شبكات الصوت والبيانات (IFCM0110)، وإدارة خدمات الإنترنت ( IFCT0509)
- متعاون خارجي CSO/SSA (كبير مسؤولي الأمن / مهندس أمني أول). جامعة Islas Baleares
- مهندس كمبيوتر. جامعة Alcalá de Henares. مدريد
- ماجستير في DevOps: Docker and Kubernetes. Cas-Training. مدريد
- تقنيات أمان Microsoft Azure. E-Council. مدريد



## الأساتذة

**أ. Armero Fernández, Rafael**

- مستشار ذكاء الأعمال في مجموعة SDG
- مهندس رقمي في Mi-GSO
- مهندس لوجيستي في Torrecid S.A
- مدرب الجودة في INDRA
- تخرج في هندسة الطيران من جامعة Politécnica في فالنسيا
- ماجستير في التطوير المهني 4.0 من جامعة Alcalá de Henares

**أ. Peris Morillo, Luis Javier**

- قائد تقني في Capitole Consulting
- مسؤول تقني ودعم رئيسي للتسليم في HCL
- مدرب ومدير العمليات في Mirai Advisory
- مطور ورئيس فريق Scrum Master Agile Coach ومدير منتج في DocPath
- هندسة كمبيوتر عليا من ESI في Ciudad Real (UCLM)
- دراسات عليا في إدارة المشاريع من قبل CEOE - الاتحاد الإسباني لمنظمات الأعمال
- أكثر من 50+ MOOCs وتدريسها من قبل جامعات معترف بها للغاية مثل جامعة Stanford وجامعة Michigan وجامعة Yonsei وجامعة Politécnica في مدريد، إلخ

**أ. Montoro Montarroso, Andrés**

- باحث في مجموعة SMILe التابعة لجامعة Castilla-La Mancha
- عالم بيانات في Prometeus Global Solutions
- شهادة في هندسة الكمبيوتر من جامعة Castilla-La Mancha في علوم الحاسوب
- ماجستير في علوم البيانات وهندسة الحاسبات من جامعة Granada

**أ. Fernández Meléndez, Galina**

- محلل بيانات في ADN Mobile Solution
- عمليات ETL، والتنقيب عن البيانات، وتحليل البيانات وتصورها، وإنشاء KPI، وتصميم وتنفيذ وثيقة التقييم، والتحكم الإداري. تطوير في برنامج R، والتعامل مع SQL، من بين أمور أخرى
- تحديد الأنماط والنماذج التنبؤية والتعلم الآلي
- بكالوريوس في إدارة الأعمال. جامعة Bicentenaria de Aragua-Caracas
- دبلوم في التخطيط والمالية العامة. المدرسة الفنزويلية في التخطيط - كلية المالية
- ماجستير في تحليل البيانات وذكاء الأعمال. جامعة Oviedo
- ماجستير في إدارة الأعمال MBA في إدارة الأعمال والإدارة (كلية إدارة الأعمال الأوروبية من برشلونة)
- ماجستير في البيانات الضخمة وذكاء الأعمال (كلية إدارة الأعمال الأوروبية من برشلونة)

**أ. Pedrajas Parabás, Elena**

- محلل أعمال في Management Solutions في مدريد
- باحثة في قسم علوم الحاسوب والتحليل العددي بجامعة قرطبة
- باحثة في مركز Centro Singular de Investigación en Tecnologías Inteligentes في سانتياغو دي كومبوستيلا
- بكالوريوس هندسة كمبيوتر. ماجستير في علوم البيانات وهندسة الحاسبات. خبرة في التدريس

**أ. Martínez Cerrato, Yésica**

- فني منتج للأمن الإلكتروني في Securitas Seguridad Spain
- محلل ذكاء الأعمال في Ricopia Technologies (جامعةAlcalá de Henares) حاصلة على شهادة في هندسة الاتصالات الإلكترونية في مدرسة Politécnica العليا، جامعة Alcalá
- مسؤول عن تدريب الموظفين الجدد فيما يتعلق ببرامج إدارة الأعمال (CRM و ERP و INTRANET) والمنتج والإجراءات في Ricopia Technologies (Alcalá de Henares)
- مسؤول عن تدريب المتدربين الجدد الذين تم دمجهم في فصول الكمبيوتر بجامعة Alcalá
- مديرة مشروع في مجال تكامل الحسابات الكبيرة في Correos y Telégrafos (مدريد)
- فني كمبيوتر - مسؤول عن فصول الكمبيوتر في OTEC بجامعة Alcalá (Alcalá de Henares)
- مدرس فصول علوم الكمبيوتر في جمعية ASALUMA (Alcalá de Henares)
- منحة للتدريب كفني كمبيوتر في OTEC بجامعة Alcalá (Alcalá de Henares)

**أ. Fondón Alcalde, Rubén**

- محلل أعمال في إدارة قيمة العملاء في شركة Vodafone Spain
- رئيس تكامل الخدمات في Entelgy for Telefónica Global Solutions
- مدير حساب عبر الإنترنت لخوادم النسخ في EDM Electronics
- محلل أعمال لجنوب أوروبا في مؤسسة Vodafone العالمية
- مهندس اتصالات من الجامعة الأوروبية بمدريد
- ماجستير في البيانات الضخمة والتحليلات من جامعة فالنسيا الدولية

**أ. Díaz Díaz-Chirón, Tobias**

- باحث في مختبر ArCO في جامعة Castilla-La Mancha وهي مجموعة مخصصة للمشاريع المتعلقة بهندسة الكمبيوتر والشبكات.
- مستشار في شركة Blue Telecomالمتخصصة في قطاع الاتصالات
- مهندس كمبيوتر أول من جامعة Castilla-La Mancha

**أ. Tato Sánchez, Rafael**

- إدارة المشروع في INDRA SISTEMAS S.A. إدارة عقد الصيانة لتركيبات أنظمة النقل الذكية التي تعتمد على مركز مراقبة الحركة وإدارتها التابع للإدارة العامة للمرور في مدريد
- مدير تقني في INDRA SISTEMAS S.A. رئيس مركز مراقبة وإدارة المرور التابع للمديرية العامة للمرور بمدريد
- مهندس أنظمة. ENA TRÁFICO S.A.
- مهندس تقني صناعي في الكهرباء من جامعة Politécnica بمدريد
- شهادة في الهندسة في الإلكترونيات الصناعية والأتمتة من جامعة مدريد الأوروبية
- شهادة احتراف. SSCE0110 التدريس للتدريب المهني للعمل
- ماجستير في الصناعة 4.0 من جامعة La Rioja الدولية (UNIR)

**أ. Catalá Barba, José Francisco**

- الإدارة الوسيطة في MINISDEF من بين مهام ومسؤوليات مختلفة داخل GOE III مثل الإدارة وإدارة الحوادث للشبكة الداخلية وتنفيذ برامج مخصصة لمناطق مختلفة ودورات تدريبية
  لشبكة المستخدمين وتجميع الموظفين بشكل عام
- فني الكتروني في مصنع Ford الموجود في Almusafes في فالنسيا وبرمجة الروبوت PLC بالإضاغة إلى الاصلاح والصيانة
- فني الكتروني
- مطور لتطبيقات الجوال

**أ. Jiménez Ramos, Álvaro**

- كبير محللي الأمن في The Workshop
- محلل الأمن السيبراني L1 في Axians
- محلل الأمن السيبراني L2 في Axians
- محلل الأمن السيبراني في SACYR S.A.
- شهادة في هندسة الاتصالات عن بعد من جامعة Politécnica بمدريد
- ماجستير في الأمن السيبراني و القرصنة الأخلاقية في CICE
- دورة عليا في الأمن السيبراني من قبل Deusto Formación

**أ. Marcos Sbarbaro, Victoria Alicia**

- مطور تطبيقات Android Mobile الأصلي في B60 المملكة المتحدة
- محلل مبرمج لإدارة وتنسيق وتوثيق البيئة الافتراضية لإنذارات أمان العميل
- محلل مبرمج لتطبيقات Java لأجهزة الصراف الآلي للعملاء
- محترف تطوير البرمجيات لتطبيق التحقق من صحة التوقيع وإدارة الوثائق للعميل
- فني أنظمة لترحيل المعدات وللإدارة والصيانة وتدريب الأجهزة المساعدة الرقمية الشخصية المحمولة للعميل
- الهندسة التقنية لأنظمة الكمبيوتر - جامعة Oberta في كاتالونيا
- درجة ماجستير في أمن الكمبيوتر و القرصنة الأخلاقية المعتمدة EC-Council و CompTIA من المدرسة المهنية للتكنولوجيات الجديدة CICE

**أ. Peralta Alonso, Jon**

- المحامي / DPO Altia للاستشاريين S.A.
- مدرس ماجستير في حماية البيانات الشخصية والأمن السيبراني وقانون تكنولوجيا المعلومات والاتصالات. الجامعة الحكومية في إقليم(Vasco (UPV-EHU
- محامي / مستشار قانوني. شركة Arriaga Associates للاستشارات القانونية والاقتصادية S.L.
- مستشار قانوني / متدرب. المكتب المهني: Oscar Padura
- شهادة بكالوريوس في القانون. الجامعة الحكومية في إقليم Vasco
- درجة ماجستير في حماية البيانات. المدرسة المبتكرة EIS
- ماجستير في القانون. الجامعة الحكومية في إقليم Vasco
- ماجستير متخصص في الإجراءات المدنية. الجامعة الدولية Isabel I de Castilla

**أ. Redondo, Jesús Serrano**

- مطور FrontEnd وفني أمن إلكتروني
- مطور الواجهة الأمامية في Telefónica بمدريد
- مطور FrontEnd. أفضل شركة استشارات احترافية SL بمدريد
- تركيب معدات وخدمات الاتصالات السلكية واللاسلكية. مجموعة Zener في Castilla و León
- تركيب معدات وخدمات الاتصالات السلكية واللاسلكية. شركة Lican للاتصالات في Castilla و León
- شهادة في أمن الحاسوب. CFTIC خيتافي، مدريد
- فني متقدم: الاتصالات السلكية واللاسلكية وأنظمة الكمبيوتر. IES Trinidad Arroyo, Palencia
- فني متقدم: التركيبات الكهروتقنية MT و BT. IES Trinidad Arroyo, Palencia
- التدريب في الهندسة العكسية والاختزال والتشفير. أكاديمية Hacker Incibe (Talentos Incibe)

05

# الهيكل والمحتوى

تم تصميم محتويات هذا الماجستير الكبير في إدارة المعلومات الآمنة مع مراعاة الحالة الحالية للمهنة بحيث يتلقى الطلاب أفضل معرفة ممكنة ويمكنهم تطبيقها في بيئة عملهم. وبالتالي من خلال الوحدات العشرين التي تشكل هذه الدرجة سيتمكن الطلاب من تعلم كل شيء عن البيانات الرقمية وإدارة المعلومات والأمن ليصبحوا متخصصين وخبراء حقيقيين في هذا المجال.

لا يوجد برنامج أفضل من هذا. يقدم لك هذا الماجستير المتقدم كل ما تحتاجه لتصبح الخبير الأول في هذه المجالات"

## الوحدة 1. تحليلات البيانات في المؤسسة التجارية

1.1. تحليل الأعمال
1.1.1. تحليل الأعمال
2.1.1. تنظيم البيانات
3.1.1. المراحل والعناصر
2.1. تحليلات البيانات في المؤسسة التجارية
1.2.1. وثائق التقييم ومؤشرات الأداء الرئيسية حسب الأقسام
2.2.1. التقارير التشغيلية والتكتيكية والاستراتيجية
3.2.1. تطبيق تحليلات البيانات على كل قسم
1.3.2.1. التسويق والاتصال
2.3.2.1. تجاري
3.3.2.1. خدمة العملاء
4.3.2.1. المشتريات
5.3.2.1. الإدارة
6.3.2.1. الموارد البشرية
7.3.2.1. الإنتاج
IT .8.3.2.1
3.1. التسويق والاتصال
1.3.1. مؤشرات الأداء الرئيسية للقياس والتطبيقات والفوائد
2.3.1. أنظمة التسويق ومخازن البيانات *Data Warehouse*
3.3.1. تنفيذ هيكل تحليل البيانات في التسويق
4.3.1. خطة التسويق والاتصال
5.3.1. الإستراتيجيات والتنبؤ وإدارة الحملات
4.1. التجارة والمبيعات
1.4.1. مساهمات تحليلات البيانات في المجال التجاري
2.4.1. احتياجات قسم المبيعات
3.4.1. دراسات السوق
5.1. خدمة العملاء
1.5.1. الولاء
2.5.1. الجودة الشخصية والذكاء العاطفي
3.5.1. رضا العملاء
6.1. المشتريات
1.6.1. تحليلات البيانات لأبحاث السوق
2.6.1. تحليلات البيانات لدراسات المنافسة
3.6.1. تطبيقات أخرى
7.1. الإدارة
1.7.1. الاحتياجات في قسم الإدارة
2.7.1. مستودع البيانات وتحليل المخاطر المالية
3.7.1. مستودع البيانات وتحليل المخاطر الائتمان
8.1. الموارد البشرية
1.8.1. الموارد البشرية وفوائد تحليلات البيانات
2.8.1. أدوات تحليل البيانات في قسم الموارد البشرية
3.8.1. تطبيق تحليلات البيانات في الموارد البشرية
9.1. الإنتاج
1.9.1. تحليل البيانات في قسم الإنتاج
2.9.1. التطبيقات
3.9.1. الفوائد
IT .10.1
1.10.1. قسم تكنولوجيا المعلومات
2.10.1. تحليلات البيانات والتحول الرقمي
3.10.1. الابتكار والإنتاجية

## الوحدة 2. إدارة ومعالجة البيانات والمعلومات لعلوم البيانات

1.2. إحصائيات. المتغيرات والمؤشرات والنسب
1.1.2. إحصائيات
2.1.2. الأبعاد الإحصائية
3.1.2. المتغيرات والمؤشرات والنسب
2.2. نوع البيانات
1.2.2. نوعية
2.2.2. كمية
3.2.2. التوصيف والفئات

3.2. معرفة البيانات من القياسات
1.3.2. تدابير المركزية
2.3.2. مقاييس التشتت
3.3.2. علاقة متبادلة
4.2. رؤى حول البيانات من الرسوم البيانية
1.4.2. التصور حسب نوع البيانات
2.4.2. تفسير المعلومات الرسومية
3.4.2. تخصيص الرسومات باستخدام برنامج آر
5.2. احتمالية
1.5.2. احتمالية
2.5.2. وظيفة الاحتمال
3.5.2. التوزيعات
6.2. جمع البيانات
1.6.2. منهجية التحصيل
2.6.2. أدوات التحصيل
3.6.2. قنوات التحصيل
7.2. تنظيف البيانات
1.7.2. مراحل تطهير البيانات
2.7.2. جودة البيانات
3.7.2. معالجة البيانات (مع برنامج آر)
8.2. تحليل البيانات وتفسيرها وتقييم النتائج
1.8.2. المقاييس الإحصائية
2.8.2. مؤشرات العلاقة
3.8.2. التنقيب في البيانات
9.2. مستودع البيانات (*Data Warehouse*)
1.9.2. عناصر
2.9.2. تصميم
10.2. توافر البيانات
1.10.2. الدخول
2.10.2. الفائدة
3.10.2. السلامة

## **الوحدة 3.** أجهزة و منصات IoT كأساس لعلوم البيانات

1.3. انترنت الأشياء
1.1.3. إنترنت المستقبل و انترنت الأشياء
2.1.3. اتحاد الإنترنت الصناعي
2.3. الهندسة المعمارية المرجعية
1.2.3. العمارة المرجعية
2.2.3. الطبقات
3.2.3. العناصر
3.3. المجسّات وأجهزة IoT
1.3.3. المكونات الرئيسية
2.3.3. المجسّات والمشغلات الميكانيكية
4.3. الاتصالات والبروتوكولات
1.4.3. بروتوكولات. نموذج OSI
2.4.3. تكنولوجيات الاتصال
5.3. المنصات السحابية لـ IoT e IIoT
1.5.3. منصات الأغراض العامة
2.5.3. منصات صناعية
3.5.3. منصات مفتوحة المصدر
6.3. إدارة البيانات في منصات إنترنت الأشياء IoT
1.6.3. آليات إدارة البيانات. البيانات المفتوحة
2.6.3. تبادل البيانات والتصور
7.3. أمن إنترنت الأشياء IoT
1.7.3. المتطلبات ومجالات الأمان
2.7.3. استراتيجيات أمان الإنترنت الصناعي للأشياء IIoT
8.3. تطبيقات إنترنت الأشياء IoT
1.8.3. المدن الذكية
2.8.3. الصحة و اللياقة
3.8.3. المنزل الذكي
4.8.3. تطبيقات أخرى

9.3. تطبيقات إنترنت الصناعي للأشياء IIoT
1.9.3. التصنيع
2.9.3. وسائل النقل
3.9.3. الطاقة
4.9.3. الزراعة والثروة الحيوانية
5.9.3. قطاعات أخرى
10.3. الصناعة 4.0
1.10.3. IoRT (إنترنت الأشياء الروبوتية)
2.10.3. تصنيع المواد المضافة ثلاثية الأبعاد
3.10.3. تحليلات البيانات الضخمة

## الوحدة 4. العرض البياني لتحليل البيانات

1.4. التحليل الاستكشافي
1.1.4. العرض من أجل تحليل المعلومات
2.1.4. قيمة التمثيل البياني
3.1.4. نماذج جديدة للتمثيل البياني
2.4. تحسين علوم البيانات
1.2.4. نطاق اللون والتصميم
2.2.4. نظرية الغَشتَلت في التمثيل البياني
3.2.4. تجنب الأخطاء والنصائح
3.4. مصادر البيانات الأساسية
1.3.4. من أجل عرض الجودة
2.3.4. من أجل عرض الكمية
3.3.4. من أجل عرض الوقت
4.4. مصادر البيانات المعقدة
1.4.4. الملفات والقوائم و BBDD
2.4.4. البيانات المفتوحة
3.4.4. إنشاء البيانات المستمرة
5.4. أنواع المخططات
1.5.4. العروض الأساسية
2.5.4. العروض الكتلية
3.5.4. العروض لتحليل التشتت
4.5.4. العروض الدائرية
5.5.4. عروض الفقاعة
6.5.4. العروض الجغرافية
6.4. أنواع العرض
1.6.4. المقارنة والعلائقية
2.6.4. توزيع
3.6.4. الهرمية
7.4. تصميم التقارير مع العرض البياني
1.7.4. تطبيق الرسوم البيانية في تقارير التسويق
2.7.4. تطبيق الرسوم البيانية في لوحات المعلومات ومؤشرات الأداء الرئيسية
3.7.4. تطبيق الرسوم البيانية في الخطط الاستراتيجية
4.7.4. استخدامات أخرى: علم، صحة، أعمال
8.4. السرد التصويري
1.8.4. السرد التصويري
2.8.4. التطور
3.8.4. الفائدة
9.4. أدوات موجهة للتصور
1.9.4. ادوات متطورة
2.9.4. برامج عبر الإنترنت
3.9.4. *Open Source*
10.4. التقنيات الجديدة في تصور البيانات
1.10.4. أنظمة لافتراضية الواقع
2.10.4. أنظمة تكبير وتقوية الواقع
3.10.4. أنظمة ذكية

## الوحدة 5. أدوات علوم البيانات

1.5. علم البيانات
1.1.5. علم البيانات
2.1.5. أدوات متقدمة لعالم البيانات
2.5. البيانات والمعلومات والمعرفة
1.2.5. البيانات والمعلومات والمعرفة
2.2.5. نوع البيانات
3.2.5. مصادر البيانات
3.5. من البيانات إلى المعلومات
1.3.5. تحليل البيانات
2.3.5. أنواع التحليل
3.3.5. استخراج المعلومات من مجموعة البيانات *Dataset*
4.5. استخراج المعلومات من خلال التصور
1.4.5. التصور كأداة تحليل
2.4.5. طرق العرض
3.4.5. عرض مجموعة البيانات
5.5. جودة البيانات
1.5.5. بيانات الجودة
2.5.5. تطهير البيانات
3.5.5. معالجة البيانات الأساسية
6.5. *Dataset*
1.6.5. إثراء مجموعة البيانات *Dataset*
2.6.5. لعنة الأبعاد
3.6.5. تعديل مجموعة البيانات الخاصة بنا
7.5. اختلال التوازن
1.7.5. عدم التوازن الطبقي
2.7.5. تقنيات تخفيف الاختلال
3.7.5. موازنة مجموعة البيانات *dataset*
8.5. نماذج غير خاضعة للرقابة
1.8.5. نموذج غير خاضع للرقابة
2.8.5. طُرق
3.8.5. التصنيف بنماذج غير خاضعة للرقابة
9.5. النماذج الخاضعة للإشراف
1.9.5. نموذج خاضع للإشراف
2.9.5. طُرق
3.9.5. التصنيف مع النماذج الخاضعة للإشراف
10.5. الأدوات والممارسات الجيدة
1.10.5. أفضل الممارسات لعالم البيانات
2.10.5. أفضل نموذج
3.10.5. أدوات مفيدة

## الوحدة 6. استخراج البيانات. الاختيار والمعالجة والتحويل

1.6. الاستدلال الإحصائي
1.1.6. الإحصاء الوصفي مقابل. الاستدلال الإحصائي
2.1.6. إجراءات حدودية
3.1.6. الإجراءات اللامعلمية
2.6. التحليل الاستكشافي
1.2.6. التحليل الوصفي
2.2.6. العرض
3.2.6. إعداد البيانات
3.6. إعداد البيانات
1.3.6. تكامل البيانات وتنقيتها
2.3.6. تطبيع البيانات
3.3.6. سمات التحويل
4.6. القيم المفقودة
1.4.6. معالجة القيم الناقصة
2.4.6. طرق التضمين القصوى
3.4.6. احتساب القيم المفقودة باستخدام التعلم الآلي
5.6. الضجيج في البيانات
1.5.6. فئات وسمات الضجيج
2.5.6. تصفية الضوضاء
3.5.6. تأثير الضجيج

6.6. لعنة الأبعاد
1.6.6. الإفراط في أخذ العينات
2.6.6. *Undersampling*
3.6.6. تقليل البيانات متعددة الأبعاد
7.6. من الصفات المستمرة إلى المنفصلة
1.7.6. البيانات المستمرة مقابل البيانات المنفصلة
2.7.6. عملية التكتم
8.6. البيانات
1.8.6. اختيار البيانات
2.8.6. وجهات النظر ومعايير الاختيار
3.8.6. مناهج الاختيار
9.6. اختيار المثيل
1.9.6. مناهج اختيار الحالات
2.9.6. اختيار النماذج
3.9.6. مناهج متقدمة لاختيار المثيل
10.6. المعالجة المسبقة للبيانات في بيئات البيانات الضخمة *Big Data*
1.10.6. البيانات الضخمة
2.10.6. المعالجة"الكلاسيكية" مقابل المعالجة المسبقة السائبة
3.10.6. *Smart Data*

## الوحدة 7. القدرة على التنبؤ وتحليل الظواهر العشوائية

1.7. السلاسل الزمنية
1.1.7. السلاسل الزمنية
2.1.7. المنفعة والتطبيق
3.1.7. الحالات ذات الصلة
2.7. السلسلة الزمنية
1.2.7. الاتجاه الموسمي ST
2.2.7. الاختلافات النموذجية
3.2.7. تحليل المخلفات
3.7. علم الأنواع
1.3.7. الثابتة
2.3.7. الغير ثابتة
3.3.7. التحولات والتعديلات
4.7. مخططات السلاسل الزمنية
1.4.7. مخطط (نموذج) مضاف
2.4.7. مخطط مضاعف (نموذج)
3.4.7. إجراءات تحديد نوع النموذج
5.7. طرق التنبؤ الأساسية *forecast*
1.5.7. نصف
2.5.7. *Naïve*
3.5.7. *Naïve* الموسمية
4.5.7. مقارنة المناهج
6.7. تحليل المخلفات
1.6.7. الارتباط التلقائي
2.6.7. النفايات ACF
3.6.7. اختبار الارتباط
7.7. الانحدار في سياق السلاسل الزمنية
1.7.7. ANOVA
2.7.7. الأساسيات
3.7.7. تطبيق عملي
8.7. النماذج التنبؤية للسلاسل الزمنية
1.8.7. ARIMA
2.8.7. تجانس الأسي
9.7. معالجة وتحليل السلاسل الزمنية باستخدام R
1.9.7. تحضير البيانات
2.9.7. تحديد النمط
3.9.7. تحليل النموذج
4.9.7. التنبؤ
10.7. الجمع بين التحليل البياني مع R
1.10.7. المواقف الإعتيادية
2.10.7. تطبيق عملي لحل المشاكل البسيطة
3.10.7. تطبيق عملي لحل المشاكل المتقدمة

## الوحدة 8. تصميم وتطوير الأنظمة الذكية

1.8. التجهيز الأولي للبيانات
1.1.8. التجهيز الأولي للبيانات
2.1.8. تحويل البيانات
3.1.8. التنقيب في البيانات
2.8. التعلم الالي
1.2.8. التعلم الخاضع للإشراف وغير الخاضع للإشراف
2.2.8. تعزيز التعلم
3.2.8. نماذج التعلم الأخرى
3.8. خوارزميات التصنيف
1.3.8. التعلم الآلي الاستقرائي
2.3.8. SVM و KNN
3.3.8. مقاييس ودرجات التصنيف
4.8. خوارزميات الانحدار
1.4.8. الانحدار الخطي والانحدار اللوجستي والنماذج غير الخطية
2.4.8. سلاسل زمنية
3.4.8. مقاييس ودرجات الانحدار
5.8. خوارزميات التجميع
1.5.8. تقنيات المجموعات الهرمية
2.5.8. تقنيات التجميع الجزئي
3.5.8. مقاييس وعشرات للتكتل *clustering*
6.8. تقنيات قواعد الرابطة
1.6.8. مناهج استخراج القواعد
2.6.8. مقاييس وعشرات خوارزميات قواعد الارتباط
7.8. تقنيات التصنيف المتقدمة. المصنفات المتعددة
1.7.8. خوارزميات التعبئة *Bagging*
2.7.8. المصنف"غابات عشوائية"*"Random Forests"*
3.7.8. لأشجار القرار*"Boosting"*
8.8. نماذج بيانية احتمالية
1.8.8. النماذج الاحتمالية
2.8.8. شبكة بايزية. الخصائص والعرض والمعلمات
3.8.8. نماذج بيانية احتمالية أخرى
9.8. الشبكات العصبية
1.9.8. التعلم الآلي مع الشبكات العصبونية الاصطناعية
2.9.8. شبكات *feedforward*
10.8. تعلم عميق
1.10.8. شبكات *feedforward* العميقة
2.10.8. الشبكات العصبونية التلافيفية ونماذج التسلسل
3.10.8. أدوات لتنفيذ الشبكات العصبية العميقة

## الوحدة 9. معماريات وأنظمة للاستخدام المكثف للبيانات

1.9. المتطلبات الغير التشغيلية ركائز تطبيقات البيانات الضخمة
1.1.9. المصداقية
2.1.9. القدرة على التكيف
3.1.9. قابلية الصيانة
2.9. نماذج البيانات
1.2.9. نموذج العلائقية
2.2.9. نموذج وثائقي
3.2.9. نموذج بيانات الرسم البياني
3.9. قواعد بيانات. تخزين البيانات وإدارة استرجاعها
1.3.9. فهارس التجزئة
2.3.9. تخزين السجل المنظم
3.3.9. بي - تري
4.9. تنسيقات ترميز البيانات
1.4.9. تنسيقات خاصة باللغة
2.4.9. تنسيقات موحدة
3.4.9. تنسيقات الترميز الثنائي
4.4.9. تدفق البيانات بين العمليات
5.9. النسخ
1.5.9. أهداف النسخ المتماثل
2.5.9. نماذج النسخ المتماثل
3.5.9. قضايا النسخ المتماثل
6.9. المعاملات الموزعة
1.6.9. العملية
2.6.9. بروتوكولات المعاملات الموزعة
3.6.9. المعاملات القابلة للتسلسل

7.9. التقسيم
1.7.9. أشكال التقسيم
2.7.9. تفاعل الفهارس الثانوية والتقسيم
3.7.9. إعادة موازنة الأقسام
8.9. معالجة البيانات دون اتصال بالإنترنت
1.8.9. تجهيز الدفعات
2.8.9. أنظمة الملفات الموزعة
3.8.9. *MapReduce*
9.9. معالجة البيانات في الوقت الحقيقي
1.9.9. أنواع وسيط الرسائل
2.9.9. تمثيل قواعد البيانات كتدفقات البيانات
3.9.9. معالجة دفق البيانات
10.9. تطبيقات عملية في المؤسسة التجارية
1.10.9. الاتساق في القراءات
2.10.9. نهج شامل للبيانات
3.10.9. توسيع نطاق الخدمة الموزعة

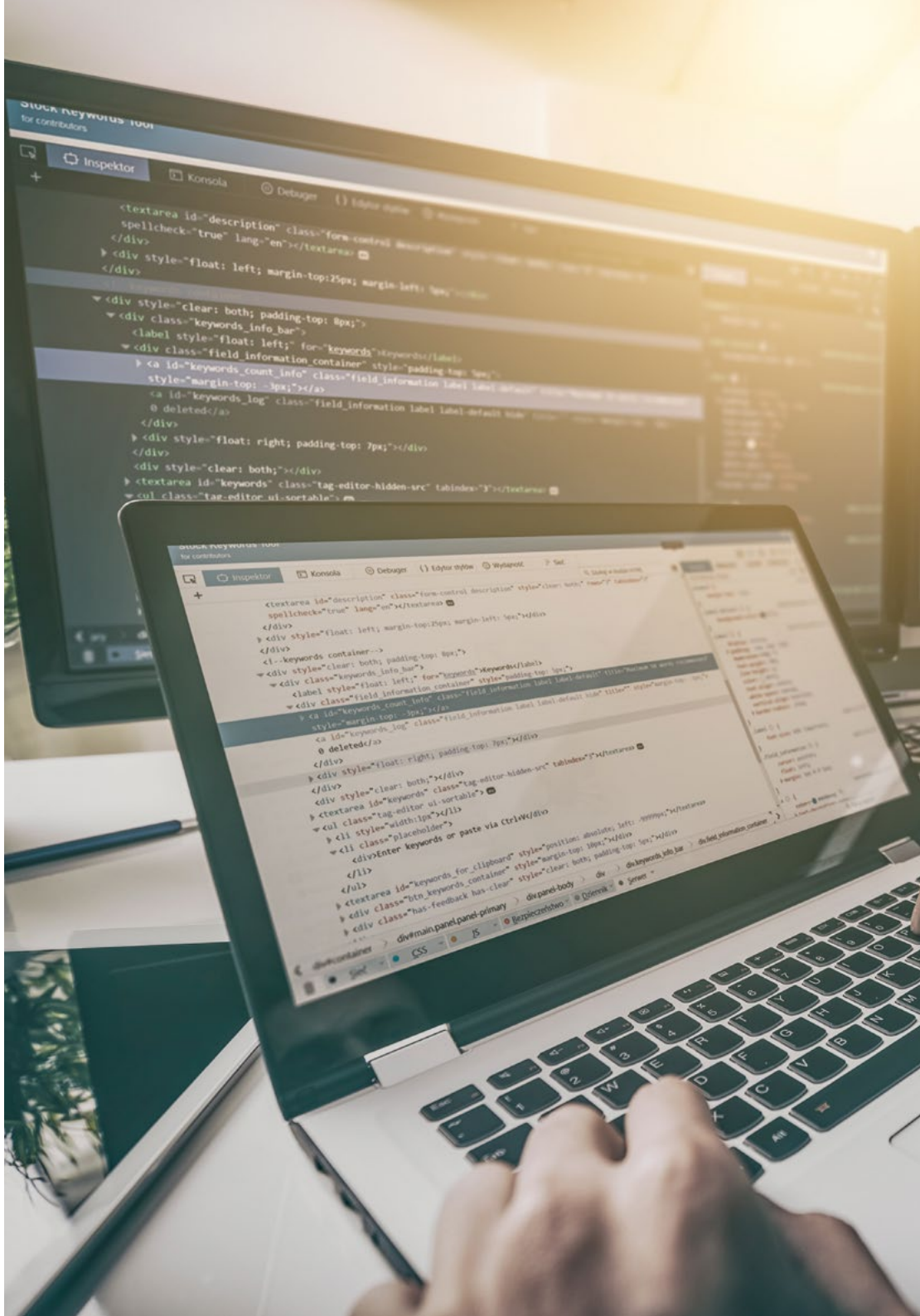
## الوحدة 10. التطبيق العملي لعلوم البيانات في قطاعات النشاط التجاري

1.10. قطاع الصحة
1.1.10. تداعيات الذكاء الاصطناعي وتحليلات البيانات في قطاع الرعاية الصحية
2.1.10. الفرص والتحديات
2.10. المخاطر والاتجاهات في قطاع الصحة
1.2.10. الاستخدام في قطاع الرعاية الصحية
2.2.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
3.10. الخدمات المالية
1.3.10. تداعيات الذكاء الاصطناعي وتحليلات البيانات في صناعة الخدمات المالية
2.3.10. الاستخدام في الخدمات المالية
3.3.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
4.10. البيع بالتجزئة Retail
1.4.10. تداعيات الذكاء الاصطناعي وتحليلات البيانات في قطاع البيع بالتجزئة
2.4.10. استخدام البيع بالتجزئة
3.4.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
5.10. الصناعة 4.0
1.5.10. تداعيات الذكاء الاصطناعي وتحليلات البيانات في الصناعة 4.0
2.5.10. الاستخدم في الصناعة 4.0
6.10. المخاطر والاتجاهات في الصناعة 4.0
1.6.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
7.10. الإدارة العامة
1.7.10. آثار الذكاء الاصطناعي وتحليلات البيانات في الإدارة العامة
2.7.10. الاستخدم في الإدارة العامة
3.7.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
8.10. تعليم
1.8.10. تداعيات الذكاء الاصطناعي وتحليلات البيانات في التعليم
2.8.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
9.10. الغابات والزراعة
1.9.10. الآثار المترتبة على الذكاء الاصطناعي وتحليلات البيانات في قطاع الغابات والزراعة
2.9.10. الاستخدم في الغابات والزراعة
3.9.10. المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي
10.10. الموارد البشرية
1.10.10 تداعيات الذكاء الاصطناعي وتحليلات البيانات في إدارة الموارد البشرية
2.10.10 تطبيقات عملية في عالم الأعمال
3.10.10 المخاطر المحتملة المتعلقة باستخدام الذكاء الاصطناعي

## الوحدة 11. الذكاء السيبراني والأمن السيبراني

1.11. الذكاء السيبراني
1.1.11. الذكاء السيبراني
2.1.1.11. الذكاء
1.2.1.1.11. دورة الذكاء
3.1.1.11. الذكاء السيبراني
4.1.1.11. الذكاء السيبراني والأمن السيبراني
2.1.11. محلل الذكاء
1.2.1.11. دور محلل الذكاء
2.2.1.11. تحيزات محلل الذكاء في النشاط التقييمي

2.11. الأمن السيبراني
1.2.11. طبقات الأمان
2.2.11. تحديد التهديدات السيبرانية
1.2.2.11. التهديدات الخارجية
2.2.2.11. التهديدات الداخلية
3.2.11. الإجراءات السلبية
1.3.2.11. الهندسة الاجتماعية
2.3.2.11. الطرق الشائعة الاستخدام
3.11. تقنيات وأدوات الذكاء
1.3.11. OSINT
2.3.11. SOCMINT
3.3.11. HUMIT
4.3.11. توزيعات وأدوات Linux
5.3.11. OWISAM
6.3.11. OWISAP
7.3.11. PTES
8.3.11. OSSTM
4.11. منهجيات التقييم
1.4.11. تحليل الذكاء
2.4.11. تقنيات تنظيم المعلومات المكتسبة
3.4.11. الموثوقية والمصداقية في مصادر المعلومات
4.4.11. منهجيات التحليل
5.4.11. عرض نتائج الاستخبارات
5.11. التدقيق والتوثيق
1.5.11. تدقيق أمن تكنولوجيا المعلومات
2.5.11. تصاريح التوثيق والتدقيق
3.5.11. أنواع التدقيق
4.5.11. التسليمات
1.4.5.11. التقرير الفني
2.4.5.11. التقرير التنفيذي
6.11. عدم الكشف عن الهوية في الشبكة
1.6.11. استخدام المجهولية
2.6.11. تقنيات إخفاء الهوية (Proxy و VPN)
3.6.11. شبكات TOR و Freenet و IP2



7.11. التهديدات وأنواع الأمن
1.7.11. أنواع التهديدات
2.7.11. الأمن المادي
3.7.11. أمن الشبكات
4.7.11. الأمن المنطقي
5.7.11. أمن تطبيقات الويب
6.7.11. أمن الجهاز المحمول
8.11. اللوائح والامتثال
1.8.11. RGPD
2.8.11. الإستراتيجية الوطنية للأمن السيبراني 2011
3.8.11. شهادة ISO 27000
4.8.11. إطار عمل الأمن السيبراني NIST
5.8.11. PIC
6.8.11. ISO 27032
7.8.11. أنظمة السحابة
8.8.11. SOX
9.8.11. PCI
9.11. تحليل المخاطر والمقاييس
1.9.11. نطاق المخاطر
2.9.11. النشطة
3.9.11. التهديدات
4.9.11. نقاط الضعف
5.9.11. تقييم المخاطر
6.9.11. علاج المخاطر
10.11. منظمات مهمة في مجال الأمن السيبراني
1.10.11. NIST
2.10.11. ENISA
3.10.11. INCIBE
4.10.11. OEA
5.10.11. UNASUR - PROSUR

## الوحدة 12. أمن المضيف

1.12. النسخ الاحتياطية
1.1.12. استراتيجيات النسخ الاحتياطي
2.1.12. أدوات لنظام التشغيل Windows
3.1.12. أدوات Linux
4.1.12. أدوات لنظام MacOS
2.12. مضاد فيروسات المستخدم
1.2.12. أنواع مضادات الفيروسات
2.2.12. مضاد فيروسات Windows
3.2.12. مضاد فيروسات Linux
4.2.12. مضاد فيروسات MacOS
5.2.12. مضاد فيروسات للهواتف الذكية
3.12. أجهزة كشف التسلل - HIDS
1.3.12. طرق كشف التطفل
2.3.12. *Sagan*
3.3.12. *Aide*
4.3.12. *Rkhunter*
4.12. جدار الحماية المحلي
1.4.12. جدار حماية Windows
2.4.12. جدار حماية Linux
3.4.12. جدار حماية MacOS
5.12. مديري كلمات المرور
1.5.12. كلمة المرور
2.5.12. *LastPass*
3.5.12. *KeePass*
4.5.12. *Sticky Password*
5.5.12. *RoboForm*
6.12. أجهزة كشف التصيدالاحتيالي
1.6.12. كشف التصيد الاحتيالي يدويا
2.6.12. أدوات مكافحة التصيد الاحتيالي

7.12. برامج التجسس
1.7.12. آليات التجنب
2.7.12. أدوات مكافحة برامج التجسس
8.12. بتتبع
1.8.12. تدابير لحماية النظام
2.8.12. أدوات مكافحة التعقب
9.12. EDR- اكتشاف نقطة النهاية والاستجابة لها
1.9.12. سلوك نظام EDR
2.9.12. الاختلافات بين EDR ومكافحة الفيروسات
3.9.12. مستقبل أنظمة EDR
10.12. السيطرة على تثبيت البرنامج
1.10.12. مستودعات ومخازن البرمجيات
2.10.12. قوائم البرامج المسموح بها أو المحظورة
3.10.12. معايير الترقية
4.10.12. امتيازات لتثبيت البرنامج

## الوحدة 13. أمان الشبكة (المحيطية)

1.13. أنظمة الكشف عن التهديدات والوقاية منها
1.1.13. الإطار العام للحوادث الأمنية
2.1.13. أنظمة الدفاع الحالية: الدفاع في العمق و SOC
3.1.13. أبنية الشبكة الحالية
4.1.13. أنواع أدوات الكشف والوقاية من الحوادث
1.4.1.13. الأنظمة القائمة على الشبكة
2.4.1.13. الأنظمة المستندة إلى المضيف
3.4.1.13. النظم المركزية
5.1.13. الاتصال واكتشاف الحالات/المضيفين والحاويات وبدون خادم
2.13. جدار الحماية
1.2.13. أنواع جدران الحماية
2.2.13. الهجمات والتخفيف منها
3.2.13. جدران الحماية الشائعة في kernel Linux
1.3.2.13. UFW
2.3.2.13. nftables و iptables
3.3.2.13. جدار الحماية
4.2.13. أنظمة الكشف على أساس سجلات النظام
1.4.2.13. مغلفات TCP
2.4.2.13. *BlockHosts* و *DenyHosts*
3.4.2.13. ban2Fai
3.13. أنظمة كشف ومنع التسلل (IDS / IPS)
1.3.13. الهجمات على IDS / IPS
2.3.13. أنظمة IDS / IPS
1.2.3.13. *Snort*
2.2.3.13. السرقاط
4.13. جدران الحماية للجيل القادم (NGFW)
1.4.13. الاختلافات بين NGFW وجدار الحماية التقليدي
2.4.13. القدرات الرئيسية
3.4.13. حلول الأعمال
4.4.13. جدران الحماية للخدمات السحابية
1.4.4.13. هندسة سحابة VPC
2.4.4.13. سحابة ACLs
3.4.4.13. مجموعة الأمان
5.13. البروكسي
1.5.13. أنواع البروكسي
2.5.13. استخدام البروكسي، المميزات والعيوب
6.13. محركات مكافحة الفيروسات
1.6.13. السياق العام للبرامج الضارة وبطاقات IOCs
2.6.13. مشاكل محرك مكافحة الفيروسات
7.13. أنظمة حماية البريد
1.7.13. مكافحة البريد المزعج
1.1.7.13. القوائم السوداء والبيضاء
2.1.7.13. فلاتر بايزي
2.7.13. بوابة البريد (MGW)
8.13. SIEM
1.8.13. المكونات والعمارة
2.8.13. قواعد الارتباط وحالات الاستخدام
3.8.13. التحديات الحالية لأنظمة SIEM

9.13. SOAR

1.9.13. SOAR و SIEM: أعداء أو حلفاء

2.9.13. مستقبل أنظمة SOAR

10.13. أنظمة أخرى قائمة على الشبكة

1.10.13. WAF

2.10.13. NAC

3.10.13. HoneyPots و HoneyNets

4.10.13. CASB

## الوحدة 14. أمان الهاتف الذكي

1.14. عالم الهواتف المحمولة

1.1.14. أنواع المنصات المتنقلة

2.1.14. أجهزة iOS

3.1.14. أجهزة Android

2.14. إدارة أمن الأجهزة المحمولة

1.2.14. مشروع OWASP للأمان على الأجهزة المحمولة

1.1.2.14. أهم 10 نقاط ضعف

2.2.14. الاتصالات والشبكات وأنماط الاتصال

3.14. الجهاز المحمول في بيئة الأعمال

1.3.14. المخاطر

2.3.14. السياسة الأمنية

3.3.14. مراقبة الجهاز

4.3.14. إدارة الأجهزة المحمولة (MDM)

4.14. خصوصية المستخدم وأمن البيانات

1.4.14. حالة المعلومات

2.4.14. حماية البيانات والسرية

1.2.4.14. أذونات

2.2.4.14. التشفير

3.4.14. تخزين آمن للبيانات

1.3.4.14. تخزين آمن في iOS

2.3.4.14. تخزين آمن في Android

4.4.14. الممارسات الجيدة في تطوير التطبيقات

5.14. نقاط الضعف ونواقل الهجوم

1.5.14. نقاط الضعف

2.5.14. نواقل الهجوم

1.2.5.14. البرمجيات الضارة

2.2.5.14. استخراج البيانات

3.2.5.14. التلاعب بالبيانات

6.14. التهديدات الرئيسية

1.6.14. مستخدم غير مقيد

2.6.14. الخبيثة

1.2.6.14. أنواع البرمجيات الضارة

3.6.14. الهندسة الاجتماعية

4.6.14. تسرب البيانات

5.6.14. سرقة المعلومات

6.6.14. شبكات *Wi-Fi* غير آمنة

7.6.14. البرمجيات الغير مُحَدَّثة

8.6.14. التطبيقات الضارة

9.6.14. كلمات السر الضعيفة

10.6.14. إعدادات الأمان ضعيفة أو غير موجودة

11.6.14. الوصول المادي

21.6.14. جهاز مفقود أو مسروق

13.6.14. انتحال الهوية (النزاهة)

14.6.14. تشفير ضعيف أو معطل

15.6.14. رفض الخدمة (DoS)

7.14. الهجمات الرئيسية

1.7.14. هجمات التصيد الاحتيالي

2.7.14. الهجمات المتعلقة بأساليب الاتصال

3.7.14. هجمات الرسائل القصيرة الاحتيالية

4.7.14. هجمات التعدين السري

5.7.14. *Man in The Middle*

8.14. القرصنة
1.8.14. التجذير وكسر الحماية
2.8.14. تشريح الهجوم المحمول
1.2.8.14. انتشار التهديد
2.2.8.14. تثبيت البرمجيات الضارة على الجهاز
3.2.8.14. المثابرة
4.2.8.14. تنفيذ الحمولة واستخراج المعلومات
3.8.14. القرصنة على أجهزة iOS: الآليات والأدوات
4.8.14. القرصنة على أجهزة Android: الآليات والأدوات
9.14. اختبارات الاختراق
1.9.14. اختبار *Pen* على *iOS*
2.9.14. اختبار *Pen* على *Android*
3.9.14. أدوات
10.14. الحماية والأمن
1.10.14. اعدادات الامان
1.1.10.14. على أجهزة iOS
2.1.10.14. على أجهزة Android
2.10.14. تدابير أمنية
3.10.14. أدوات الحماية

## الوحدة 15. أمن إنترنت الأشياء IoT

1.15. الأجهزة
1.1.15. أنواع الأجهزة
2.1.15. أبنية موحدة
1.2.1.15 M2ONEM
2.2.1.15 IoTWF
3.1.15. بروتوكولات التطبيق
4.1.15. تقنيات الاتصال
2.15. أجهزة IoT. مجالات التطبيق
1.2.15. المنزل الذكي
2.2.15. المدينة الذكية
3.2.15. وسائل النقل
4.2.15. الأجهزة القابلة للارتداء
5.2.15. القطاع الصحي
6.2.15 IioT

3.15. بروتوكولات الاتصال
1.3.15 MQTT
2.3.15 LWM2M
3.3.15 OMA-DM
4.3.15 -TR069
4.15. المنزل الذكي
1.4.15. التشغيل الآلي للمنزل
2.4.15. شبكات التواصل
3.4.15. الأجهزة المنزلية
4.4.15. اليقظة والأمن
5.15. المدينة الذكية
1.5.15. الإضاءة
2.5.15. علم الارصاد الجوية
3.5.15. السلامة
6.15. وسائل النقل
1.6.15. موقع
2.6.15. سداد المدفوعات والحصول على الخدمات
3.6.15. الاتصال
7.15. الأجهزة القابلة للارتداء
1.7.15. الملابس الذكية
2.7.15. المجوهرات الذكية
3.7.15. الساعات الذكية
8.15. القطاع الصحي
1.8.15. التمرين / مراقبة معدل ضربات القلب
2.8.15. مراقبة المرضى وكبار السن
3.8.15. الزرع
4.8.15. الروبوتات الجراحية
9.15. الاتصال
1.9.15. شبكة *WiFi* / البوابة الالكترونية
2.9.15. *Bluetooth*
3.9.15. اتصال مدمج

10.15. التوريق

1.10.15. شبكات مخصصة

2.10.15. مسئول كلمات المرور

3.10.15. استخدام البروتوكولات المشفرة

4.10.15. استخدم النصائح

## الوحدة 16. القرصنة الأخلاقية

1.16. بيئة العمل

1.1.16. توزيعات Linux

1.1.1.16. Kali Linux - الحماية الهجومية

2.1.1.16. نظام تشغيل Parrot

3.1.1.16. Ubuntu

2.1.16. أنظمة المحاكاة الافتراضية

3.1.16. *Sandbox*

4.1.16. انتشار المعامل

2.16. المنهجيات

1.2.16. OSSTM

2.2.16. OWASP

3.2.16. NIST

4.2.16. PTES

5.2.16. ISSAF

3.16. البصمات

1.3.16. استخبارات مفتوحة المصدر (OSINT)

2.3.16. البحث عن خرق البيانات ونقاط الضعف

3.3.16. استخدام الأدوات الخاملة

4.16. فحص الشبكة

1.4.16. أدوات المسح

1.1.4.16. Nmap

2.1.4.16. Hping3

3.1.4.16. أدوات المسح الأخرى

2.4.16. تقنيات المسح

3.4.16. تقنيات التهرب من جدار الحماية و IDS

4.4.16. لافتة الاستيلاء

5.4.16. مخططات الشبكة

5.16. ترقيم

1.5.16. ترقيم SMTP

2.5.16. ترقيم DNS

3.5.16. ترقيم NetBIOS و Samba

4.5.16. ترقيم LDAP

5.5.16. ترقيم SNMP

6.5.16. تقنيات الترقيم الأخرى

6.16. فحص الثغرات الأمنية

1.6.16. حلول لفحص الثغرات الأمنية

1.1.6.16. Qualys

2.1.6.16. Nessus

3.1.6.16. CFI LanGuard

2.6.16. أنظمة تسجيل الثغرات الأمنية

1.2.6.16. CVSS

2.2.6.16. CVE

3.2.6.16. NVD

7.16. الهجمات على الشبكات اللاسلكية

1.7.16. منهجية القرصنة في الشبكات اللاسلكية

1.1.7.16. اكتشاف شبكة *WiFi*

2.1.7.16. تحليل الحركة

3.1.7.16. هجمات *Aircrack*

1.3.1.7.16. هجمات الويب

2.3.1.7.16. هجمات WPA2 / WPA

4.1.7.16. هجمات *EvilTwin*

5.1.7.16. هجمات WPS

6.1.7.16. *Jamming*

2.7.16. أدوات الأمن اللاسلكية

8.16. قرصنة خادم الويب

1.8.16. البرمجة عبر الموقع

2.8.16. CSRF

3.8.16. قرصنة الجلسة

4.8.16. *SQLinjection*

9.16. استغلال الثغرات الأمنية

1.9.16. استخدام الثغرات المعروفة

2.9.16. استخدام ميتاسبلويت

3.9.16. استخدام البرمجيات الضارة

1.3.9.16. التعريف والنطاق

2.3.9.16. إنشاء البرمجيات الضارة

3.3.9.16. تجاوز حلول الحماية من الفيروسات

10.16. المثابرة

1.10.16. تركيب الجذور الخفية

2.10.16. استخدام ncat

3.10.16. استخدام المهام المجدولة ل backdoors

4.10.16. إنشاء المستخدمين

5.10.16. الكشف عن HIDS

## الوحدة 17. الهندسة العكسية

1.17. المُجَمِعين

1.1.17. أنواع الأكواد أو الرموز

2.1.17. أطوار المترجم

3.1.17. جدول الرموز

4.1.17. معالج الأخطاء

5.1.17. مترجم GCC

2.17. أنواع التحليل في المجمعين

1.2.17. التحليل المعجمي

1.1.2.17. المصطلحات

2.1.2.17. المكونات المعجمية

3.1.2.17. محلل LEX المعجمي

2.2.17. التحليل النحوي

1.2.2.17. القواعد النحوية الخالية من السياق

2.2.2.17. أنواع التحليل

1.2.2.2.17. التحليل التنازلي

2.2.2.2.17. التحليل التصاعدي

3.2.2.17. أشجار النحو والاشتقاقات

4.2.2.17. أنواع المحللات

1.4.2.2.17. أجهزة التحليل LR (من اليسار إلى اليمين)

2.4.2.2.17. محللات LALR

3.2.17. التحليل الدلالي

1.3.2.17. السمة النحوية

2.3.2.17. المنسوبات-S

3.3.2.17. المنسوبات-L

3.17. هياكل البيانات في المُجمّع

1.3.17. المتغيرات

2.3.17. المصفوفات

3.3.17. المؤشرات

4.3.17. الهياكل

5.3.17. العناصر

4.17. هياكل كود التجميع

1.4.17. هياكل الاختيار

1.1.4.17. If, else if, Else

2.1.4.17. Switch

2.4.17. هياكل التكرار

1.2.4.17. For

2.2.4.17. While

3.2.4.17. استخدام كسر التكرار البرمجي break

3.4.17. المهام

5.17. هندسة الأجهزة في x86

1.5.17. هندسة المعالجات في x86

2.5.17. هياكل البيانات في x86

3.5.17. هياكل الكود في x86

6.17. هندسة الأجهزة في ARM

1.6.17. هندسة المعالجات في ARM

2.6.17. هياكل البيانات في ARM

3.6.17. هياكل الكود في ARM

7.17. تحليل الكود الثابت

1.7.17. المفككات

2.7.17. IDA

3.7.17. مصممي الكود

8.17. تحليل الكود الديناميكي

1.8.17. تحليل السلوك

1.1.8.17. الاتصالات

2.1.8.17. المتابعة

2.8.17. مصححات التعليمات البرمجية على Linux

3.8.17. مصححات التعليمات البرمجية على Windows

9.17. *Sandbox*

1.9.17. هندسة تصميم *Sandbox*

2.9.17. التهرب من *Sandbox*

3.9.17. تقنيات الكشف

4.9.17. تقنيات التهرب

5.9.17. التدابير المضادة

6.9.17. *Sandbox* في Linux

7.9.17. *Sandbox* في Windows

8.9.17. *Sandox* في MacOS

9.9.17. *Sandbox* في Android

10.17. تحليل البرمجيات الخبيثة

1.10.17. تحليل البرمجيات الضارة

2.10.17. تقنيات التعتيم على البرمجيات الضارة

1.2.10.17. التعتيم على الملفات التنفيذية

2.2.10.17. تقييد بيئات التنفيذ

3.10.17. أدوات تحليل البرمجيات الضارة

## الوحدة 18. التنمية الآمنة

1.18. التنمية الآمنة

1.1.18. الجودة والأداء والسلامة

2.1.18. السرية والنزاهة والتوافر

3.1.18. دورة حياة تطوير البرمجيات

2.18. مرحلة المتطلبات

1.2.18. مراقبة المصادقة

2.2.18. السيطرة على الأدوار والامتيازات

3.2.18. المتطلبات الموجهة نحو المخاطر

4.2.18. الموافقة على الامتياز

3.18. مراحل التصميم والتحليل

1.3.18. الوصول إلى المكونات وإدارة النظام

2.3.18. مسارات مراجعة الحسابات

3.3.18. إدارة الجلسة

4.3.18. الحقائق التاريخية

5.3.18. المعالجة المناسبة للخطأ

6.3.18. فصل المهمات

4.18. مرحلة التنفيذ والترميز

1.4.18. ضمان بيئة التطوير

2.4.18. إعداد الوثائق الفنية

3.4.18. التشفير الآمن

4.4.18. أمن الإتصالات

5.18. ممارسات الترميز الآمنة الجيدة

1.5.18. التحقق من صحة البيانات المدخلة

2.5.18. ترميز بيانات الإخراج

3.5.18. أسلوب البرمجة

4.5.18. تغيير معالجة السجل

5.5.18. التدرب على التشفير

6.5.18. الخطأ وإدارة السجل

7.5.18. إدارة الملفات

8.5.18. إدارة الذاكرة

9.5.18. توحيد وإعادة استخدام وظائف الأمن

6.18. إعداد الخادم و تقوية
1.6.18. إدارة المستخدمين والمجموعات والأدوار على الخادم
2.6.18. تنصيب البرامج
3.6.18. تقوية الخادم
4.6.18. التكوين المتين لبيئة التطبيق
7.18. اعداد قاعدة البيانات و تقوية
1.7.18. تحسين محرك قاعدة البيانات
2.7.18. إنشاء المستخدم الخاص للتطبيق
3.7.18. تعيين الامتيازات الدقيقة للمستخدم
4.7.18. تقوية قاعدة البيانات
8.18. مرحلة الإختبار
1.8.18. مراقبة الجودة في الضوابط الأمنية
2.8.18. فحص الكود المرحلي
3.8.18. فحص إدارة التكوين
4.8.18. اختبار الصندوق الأسود
9.18. التحضير للانتقال إلى الإنتاج
1.9.18. قم بمراقبة التغيير
2.9.18. قم بتنفيذ إجراءات خطوة الإنتاج
3.9.18. تنفيذ إجراء العودة إلى الحالة السابقة
4.9.18. الاختبارات في مرحلة ما قبل الإنتاج
10.18. مرحلة الصيانة
1.10.18. التأكيد على أساس المخاطر
2.10.18. اختبار صيانة الصندوق الأبيض
3.10.18. اختبار صيانة الصندوق الأسود

## الوحدة 19. تحليل الطب الشرعي

1.19. الحصول على البيانات والازدواجية
1.1.19. الحصول على البيانات المتقلبة
1.1.1.19. معلومات النظام
2.1.1.19. معلومات الشبكة
3.1.1.19. ترتيب التقلب
2.1.19. الحصول على البيانات الثابتة
1.2.1.19. عمل نسخة طبق الأصل
2.2.1.19. إعداد وثيقة لسلسلة الحراسة
3.1.19. طرق التحقق من صحة البيانات المكتسبة
1.3.1.19. طرق Linux
2.3.1.19. طرق Windows
2.19. تقييم وهزيمة تقنيات مكافحة الأدلة الجنائية
1.2.19. أهداف تقنيات مكافحة الأدلة الجنائية
2.2.19. حذف البيانات
1.2.2.19. حذف البيانات والملفات
2.2.2.19. استعادة الملف
3.2.2.19. استعادة الأجزاء المحذوفة
3.2.19. حماية كلمة المرور
4.2.19. إخفاء المعلومات
5.2.19. محو بيانات الجهاز الآمن
6.2.19. التشفير
3.19. التحليل الجنائي لنظام التشغيل
1.3.19. التحليل الجنائي لنظام Windows
2.3.19. التحليل الجنائي لنظام Linux
3.3.19. التحليل الجنائي لنظام Mac
4.19. التحليل الجنائي للشبكة
1.4.19. تحليل السجلات
2.4.19. ارتباط البيانات
3.4.19. التحقيق ضمن الشبكة
4.4.19. خطوات لمتابعة التحليل الجنائي للشبكة
5.19. التحليل الجنائي للويب
1.5.19. التحقيق في الهجمات على الويب
2.5.19. الكشف عن الهجوم
3.5.19. موقع عناوين بروتوكول الإنترنت IPs
6.19. قاعدة بيانات التحليل الجنائي
1.6.19. التحليل الجنائي في MSSQL
2.6.19. التحليل الجنائي في MySQL
3.6.19. التحليل الجنائي في PostgreSQL
4.6.19. التحليل الجنائي في MongoDB

7.19. التحليل الجنائي في السحابية

1.7.19. أنواع الجرائم السحابية

1.1.7.19. السحابة كعنصر

2.1.7.19. السحابة ككائن

3.1.7.19. السحابة كأداة

2.7.19. تحديثات التحليل الجنائي للسحابة

3.7.19. التحقيق في خدمات التخزين للسحابية

4.7.19. أدوات التحليل الجنائي للسحابة

8.19. التحقيق في الجرائم عبر البريد الإلكتروني

1.8.19. أنظمة البريد

1.1.8.19. عملاء البريد

2.1.8.19. خادم البريد

3.1.8.19. خادم SMTP

4.1.8.19. خادم POP3

5.1.8.19. خادم IMAP4

2.8.19. جرائم البريد

3.8.19. رسائل البريد الإلكتروني

1.3.8.19. الرؤوس القياسية

2.3.8.19. الرؤوس الموسعة

4.8.19. خطوات التحقيق في هذه الجرائم

5.8.19. أدوات جنائية للبريد الإلكتروني

9.19. التحليل الجنائي لنظام المحمول

1.9.19. الشبكات الخلوية

1.1.9.19. أنواع الشبكات

2.1.9.19. محتويات CDR

2.9.19. وحدة تعريف المشترك (SIM)

3.9.19. الاستحواذ المنطقي

4.9.19. الاستحواذ المادي

5.9.19. الحصول على نظام الملفات

10.19. صياغة وتقديم التقارير للتحاليل الجنائية

1.10.19. جوانب مهمة من تقرير للتحاليل الجنائية

2.10.19. تصنيف وأنواع التقارير

3.10.19. دليل لكتابة التقرير

4.10.19. عرض التقرير

1.4.10.19. التحضير السابق للشهادة

2.4.10.19. الإيداع

3.4.10.19. التعامل مع وسائل الإعلام

## الوحدة 20. التحديات الحالية والمستقبلية في أمن الكمبيوتر

1.20. تقنية *Blockchain*

1.1.20. مجالات التطبيق

2.1.20. ضمان السرية

3.1.20. ضمان عدم الرفض

2.20. النقود الرقمية

1.2.20. بيتكوين

2.2.20. العملات الرقمية

3.2.20. تعدين العملات المشفرة

4.2.20. مخططات بونزي

5.2.20. الجرائم والمشاكل المحتملة الأخرى

3.20. التزييف العميق

1.3.20. تأثير وسائل الإعلام

2.3.20. الأخطار على المجتمع

3.3.20. آليات الكشف

4.20. مستقبل الذكاء الاصطناعي

1.4.20. الذكاء الاصطناعي والحوسبة المعرفية

2.4.20. الاستخدامات لتبسيط خدمة العملاء

5.20. الخصوصية الرقمية

1.5.20. قيمة البيانات في الشبكة

2.5.20. استخدام البيانات على الشبكة

3.5.20. إدارة الخصوصية والهوية الرقمية

6.20. النزاعات السيبرانية ومجرمو الإنترنت والهجمات الإلكترونية
1.6.20. تأثير الأمن السيبراني في النزاعات الدولية
2.6.20. عواقب الهجمات الإلكترونية على عموم السكان
3.6.20. أنواع مجرمي الإنترنت. تدابير الحماية
7.20. العمل إلكترونيا
1.7.20. ثورة العمل عن بعد أثناء وبعد Covid19
2.7.20. اختناقات الوصول
3.7.20. تباين سطح الهجوم
4.7.20. احتياجات العامل
8.20. التقنيات اللاسلكية الناشئة
1.8.20. WPA3
2.8.20. 5G
3.8.20. موجات ملليمتر
4.8.20. الاتجاه في "*Get Smart*" بدلاً من "*Get more*"
9.20. عنونة المستقبل في الشبكات
1.9.20. المشكلات الحالية مع معالجة IP
2.9.20. IPv6
2.9.20. +IPv4
3.9.20. مزايا IPv4 + عبر IPv4
4.9.20. مزايا IPv6 عبر IPv4
10.20. التحدي المتمثل في زيادة الوعي بالتدريب المبكر والمستمر للسكان
1.10.20. الاستراتيجيات الحكومية الحالية
2.10.20. المقاومة السكانية للتعلم
3.10.20. خطط التدريب التي يجب أن تتبناها الشركات

"لا تفكر طويلا، لأنك تدرك أنك مع هذا الماجيستير المتقدم ستصل إلي أبعد ما يكون"

06

# المنهجية

يقدم هذا البرنامج التدريبي طريقة مختلفة للتعلم. تم تطوير منهجيتنا من خلال وضع التعلم الدوري: إعادة التعلم.

يُستخدم نظام التدريس هذا، على سبيل المثال، في أرقى كليات الطب في العالم، وقد تم اعتباره من أكثر الكليات فعالية من خلال المنشورات ذات الأهمية الكبيرة مثلمجلة نيو إنجلاند الطبية.

اكتشف إعادة التعلم، وهو نظام يتخلى عن التعلم الخطي التقليدي ليأخذك من خلال أنظمة التدريس الدورية: طريقة تعلم أثبتت فعاليتها الهائلة، خاصة في الموضوعات التي تتطلب الحفظ "

### دراسة حالة لوضع جميع المحتويات في سياقها

يقدم برنامجنا طريقة ثورية لتطوير المهارات والمعرفة. هدفنا هو تعزيز الكفاءات في سياق متغير وتنافسي وعالي الطلب.

مع تيك يمكنك تجربة طريقة للتعلم تعمل على تحريك أسس الجامعات التقليدية في جميع أنحاء العالم"


سوف تصل إلى نظام تعليمي قائم على التكرار ، مع تدريس طبيعي وتقدمي في جميع أنحاء المنهج الدراسي بأكمله

سيتعلم الطالب،من خلال الأنشطة التعاونية والحالات الحقيقية،حل المواقف المعقدة في بيئات الأعمال الحقيقية.

## طريقة تعلم م بتكرة ومختلفة

برنامج تيك الحالي هو تعليم مكثف ، تم إنشاؤه من الصفر ، والذي يقترح التحديات والقرارات الأكثر تطلبًا في هذا المجال، سواء على المستوى المحلي أو الدولي. بفضل هذه المنهجية يتم تعزيز النمو الشخصي والمهني ، واتخاذ خطوة حاسمة نحو النجاح. طريقة الحالة ، تقنية تضع الأسس لهذا المحتوى ، تضمن اتباع أحدث واقع اقتصادي واجتماعي ومهني.

> برنامجنا يعدك لمواجهة تحديات جديدة في بيئات غير مؤكدة وتحقيق النجاح في حياتك المهنية "

كانت طريقة الحالة هي نظام التعلم الأكثر استخدامًا من قبل أفضل مدارس نظم المعلومات في العالم منذ وجودها. تم تطويره في عام 1912 بحيث لا يتعلم طلاب القانون القوانين بناءً على المحتويات النظرية فحسب بل كانت طريقة القضية هي تقديم مواقف معقدة حقيقية لهم لاتخاذ قرارات مستنيرة وتقدير الأحكام حول كيفية حلها. في عام 1924 تم تأسيسها كطريقة معيارية للتدريس في جامعة هارفارد.

في موقف محدد ، ما الذي يجب أن يفعله المحترف؟ هذا هو السؤال الذي نواجهه في أسلوب الحالة ، وهو أسلوب التعلم العملي. خلال البرنامج ، سيواجه الطلاب حالات حقيقية متعددة. يجب عليهم دمج كل معارفهم والتحقيق والمناقشة والدفاع عن أفكارهم وقراراتهم.

## منهجية إعادة التعلم

تجمع تيك بفعالية بين منهجية دراسة الحالة ونظام تعلم عبر الإنترنت بنسبة 100٪ استنادًا إلى التكرار ، والذي يجمع بين عناصر تعليمية مختلفة في كل درس.

نحن نشجع دراسة الحالة بأفضل طريقة تدريس بنسبة 100٪:عبر الإنترنت  إعادة التعلم.


في عام *2019* ، حصلنا على أفضل نتائج تعليمية لجميع الجامعات عبر الإنترنت باللغة الإسبانية في العالم

في تيك تتعلم بمنهجية طليعية مصممة لتدريب مديري المستقبل. هذه الطريقة ، في طليعة التعليم العالمي ، تسمى إعادة التعلم.

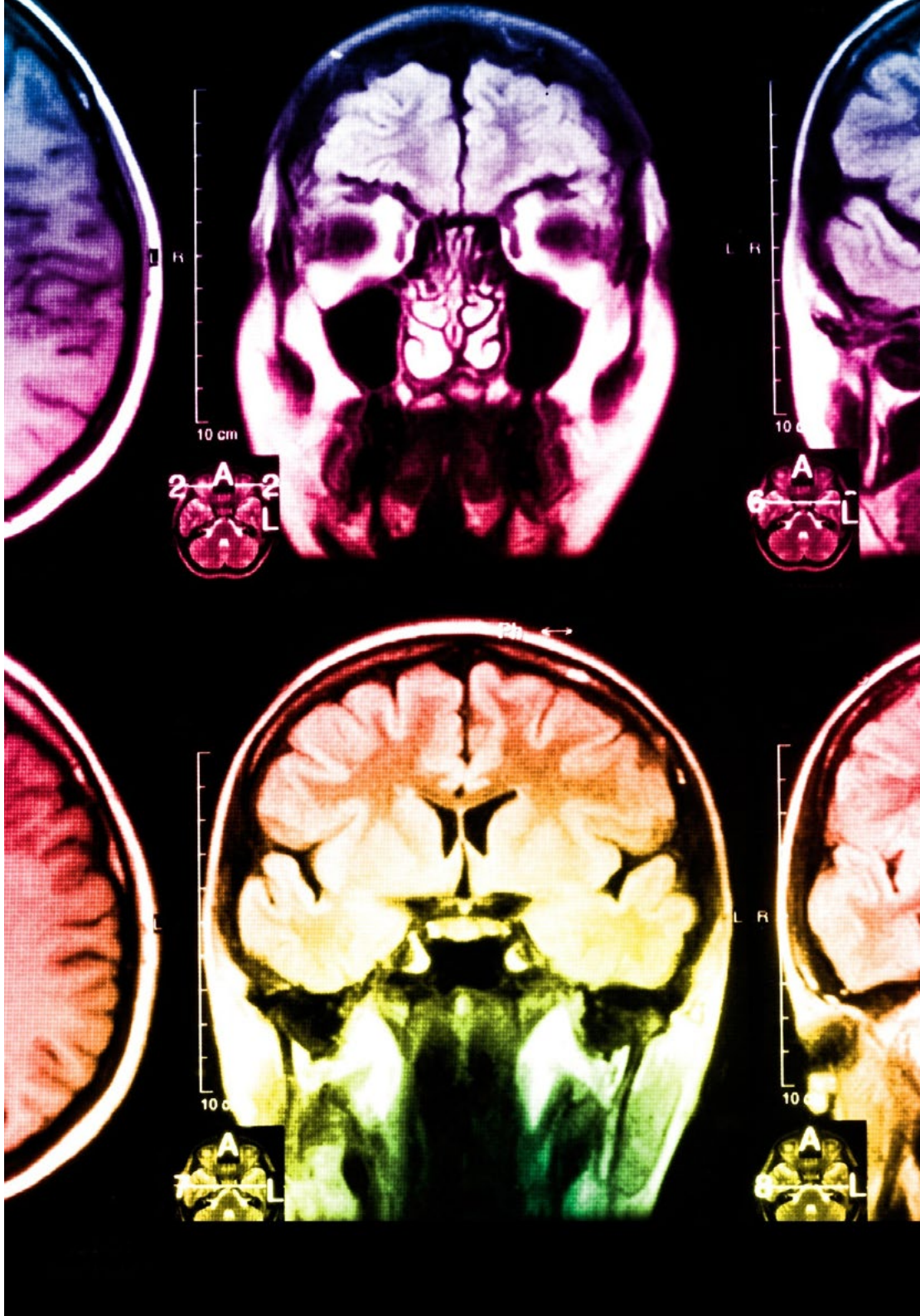
جامعتنا هي الجامعة الوحيدة الناطقة بالإسبانية المرخصة لاستخدام هذه الطريقة الناجحة. في عام 2019 ، تمكنا من تحسين مستويات الرضا العام لطلابنا )جودة التدريس ، جودة المواد ، هيكل الدورة ، الأهداف.... (فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

في برنامجنا ، التعلم ليس عملية خطية ، ولكنه يحدث في دوامة )تعلم ، وإلغاء التعلم ، والنسيان ، وإعادة التعلم(. لذلك ، يتم دمج كل عنصر من هذه العناصر بشكل مركز. باستخدام هذه المنهجية ، تم تدريب أكثر من 650 ألف خريج جامعي بنجاح غير مسبوق في مجالات متنوعة مثل الكيمياء الحيوية ، وعلم الوراثة ، والجراحة ، والقانون الدولي ، والمهارات الإدارية ، وعلوم الرياضة ، والفلسفة ، والقانون ، والهندسة ، والصحافة ، والتاريخ ، والأسواق والأدوات المالية. كل هذا في بيئة يرتفع فيها ،الطلب مع طالب جامعي يتمتع بمكانة اجتماعية واقتصادية عالية ومتوسط عمر 43.5 سنة

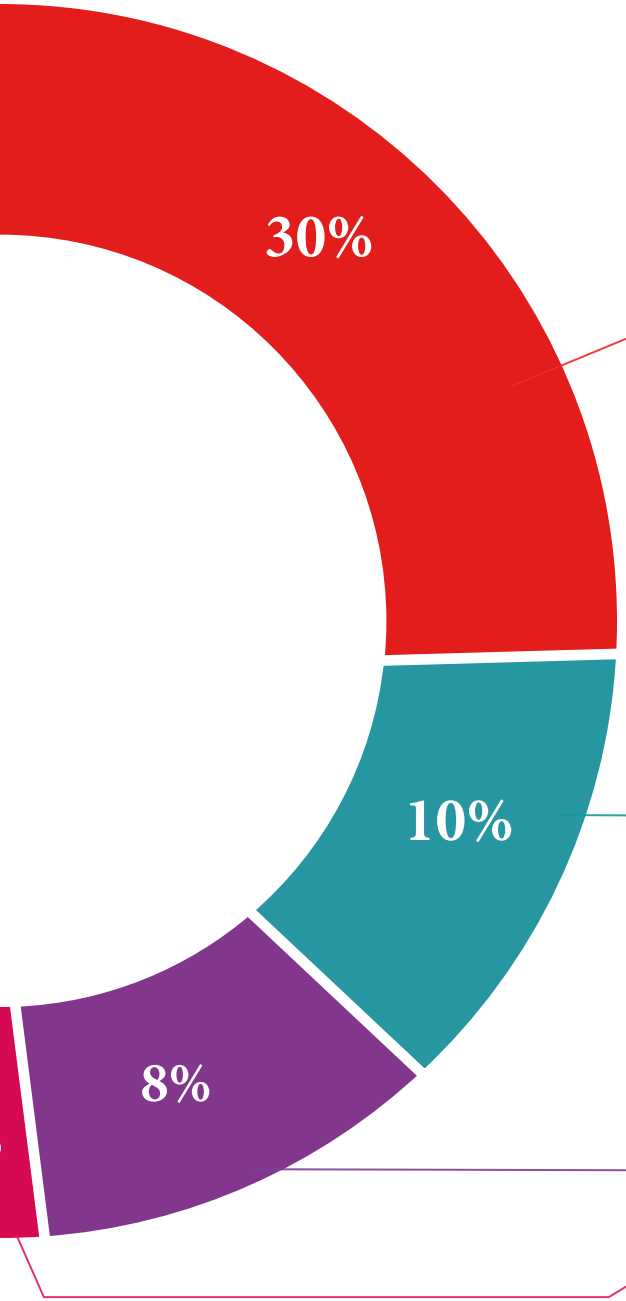
ستسمح لك إعادة التعلم بالتعلم بجهد أقل وأداء أكبر ، والمشاركة بشكل أكبر في تدريبك ، وتنمية الروح النقدية ، والدفاع عن الحجج والآراء المتناقضة: معادلة مباشرة للنجاح.

استنادًا إلى أحدث الأدلة العلمية في مجال علم الأعصاب ، لا نعرف فقط كيفية تنظيم المعلومات والأفكار والصور والذكريات ، ولكننا نعلم أيضًا أن المكان والسياق الذي تعلمنا فيه شيئًا ضروريًا لنا لنكون قادرين على ذلك. تذكرها وتخزينها في قرن آمون ، للاحتفاظ بها في ذاكرتنا طويلة المدى

بهذه الطريقة ، وفيما يسمى التعلم الإلكتروني المعتمد على السياق العصبي ، ترتبط العناصر المختلفة لبرنامجنا بالسياق الذي يطور فيه المشارك ممارسته المهنية



**يقدم هذا البرنامج أفضل المواد التعليمية المعدة بعناية للمحترفين:**




### المواد الدراسية

تم إنشاء جميع المحتويات التعليمية من قبل المتخصصين الذين سيقومون بتدريس الدورة ، خاصةً له ، بحيث يكون التطوير التعليمي محددًا وملموسًا حقًا.

يتم تطبيق هذه المحتويات بعد ذلك على التنسيق السمعي البصري ، لإنشاء طريقة عمل تيك عبر الإنترنت. كل هذا ، مع أكثر التقنيات ابتكارًا التي تقدم قطعًا عالية الجودة في كل مادة من المواد التي يتم توفيرها للطالب.

### فصول الماجستير

هناك أدلة علمية على فائدة ملاحظة طرف ثالث من الخبراء.

ما يسمى التعلم من خبير يقوي المعرفة والذاكرة ، ويولد الأمان في القرارات الصعبة في المستقبل.

### ممارسات المهارات والكفاءات

سيقومون بتنفيذ أنشطة لتطوير مهارات وقدرات محددة في كل مجال موضوعي. الممارسات والديناميكيات لاكتساب وتطوير المهارات والقدرات التي يحتاج المتخصص إلى تطويرها في إطار العولمة التي نعيشها.

### قراءات تكميلية

مقالات حديثة ووثائق إجماع وإرشادات دولية ، من بين أمور أخرى. في مكتبة تيك الافتراضية ، سيتمكن الطالب من الوصول إلى كل ما يحتاجه لإكمال تدريبه.

### دراسات الحالة

سوف يكملون مجموعة مختارة من أفضل دراسات الحالة المختارة بالتحديد لهذا المؤهل. الحالات التي تم عرضها وتحليلها وتدريسها من قبل أفضل المتخصصين على الساحة الدولية

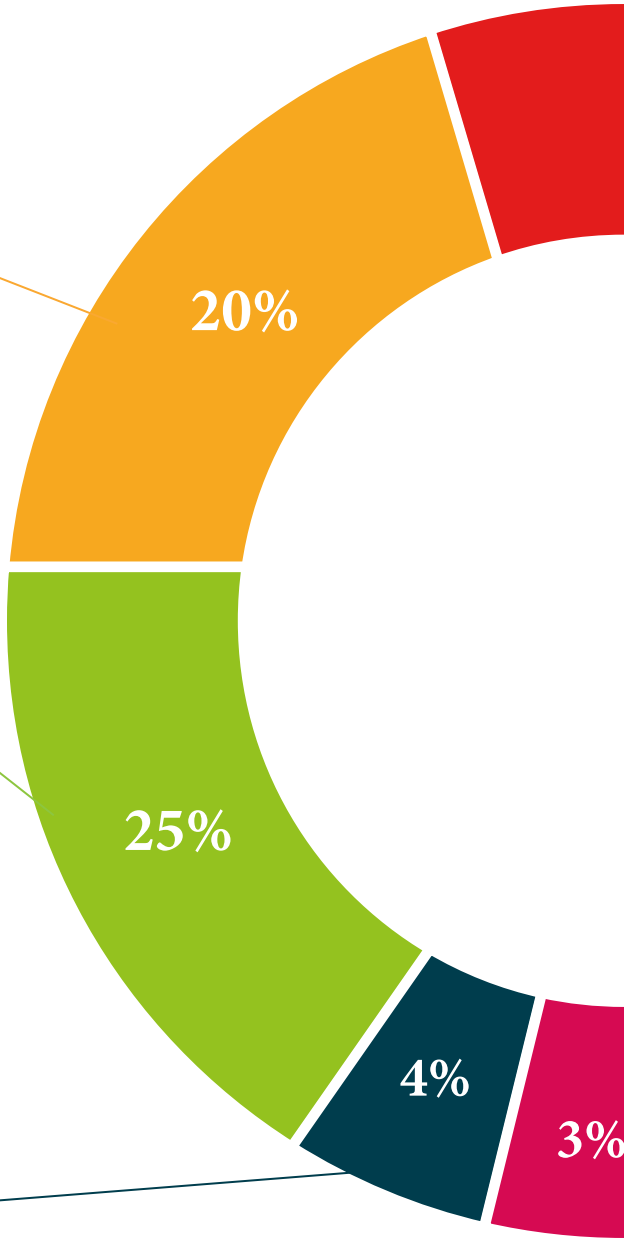
### ملخصات تفاعلية

يقدم فريق تيك المحتوى بطريقة جذابة وديناميكية في أقراص المحتوى بطريقة جذابة وديناميكية في أقراص الوسائط المتعددة التي تشمل الصوت والفيديو والصور والرسوم البيانية والخرائط المفاهيمية من أجل تعزيز المعرفة

تم منح هذا النظام التعليمي الحصري الخاص بتقديم محتوى الوسائط المتعددة من قبل شركة Microsoft كـ "حالة نجاح في أوروبا"

### الاختبار وإعادة الاختبار

يتم تقييم معرفة الطالب بشكل دوري وإعادة تقييمها في جميع أنحاء البرنامج ، من خلال أنشطة وتمارين التقييم الذاتي والتقويم الذاتي بحيث يتحقق الطالب بهذه الطريقة من كيفية تحقيقه لأهدافه



07

# المؤهل العلمي

يضمن الماجستير المتقدم في إدارة المعلومات الآمنة إلى التدريب الأكثر صرامة وحداثة والحصول على شهادة جامعية صادرة عن TECH الجامعة التكنولوجية.

أكمل هذا البرنامج بنجاح واحصل على شهادتك الجامعية دون السفر أو الأعمال المرهقة"

تحتوي درجة **الماجستير المتقدم في إدارة المعلومات الآمنة** على البرنامج العلمي الأكثر اكتمالا وحداثة في السوق.

بعد اجتياز الطالب للتقييمات، سوف يتلقى عن طريق البريد العادي* مصحوب بعلم وصول مؤهل **الماجستير المتقدم** ذا الصلة الصادرة عن **الجامعة التكنولوجية TECH.**

إن المؤهل الصادر عن **TECH الجامعة التكنولوجية** سوف يشير إلى التقدير الذي تم الحصول عليه في الماجستير المتقدم وسوف يفي بالمتطلبات التي عادة ما تُطلب من قبل مكاتب التوظيف ومسابقات التعيين ولجان التقييم الوظيفي والمهني.

المؤهل العلمي: **ماجستير متقدم في إدارة المعلومات الآمنة**

عدد الساعات الدراسية المعتمدة: **3.000 ساعة**


الجامعة التكنولوجية

تمنح هذا

الدبلوم

لـ

المواطن/المواطنة ..... مع وثيقة تحقيق شخصية رقم .....

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

ماجستير متقدم

في

إدارة المعلومات الآمنة

وهي شهادة خاصة من هذه الجامعة موافقة لـ 3.000 ساعة، مع تاريخ بدء يوم/شهر/ سنة وتاريخ انتهاء يوم/شهر/سنة

تيك مؤسسة خاصة للتعليم العالي معتمدة من وزارة التعليم العام منذ 28 يونيو 2018

في تاريخ 17 يونيو 2020

أ. د./ Tere Guevara Navarro

رئيس الجامعة

الكود الفريد الخاص بجامعة TECH: AFWOR23S techtitute.com/certificates


ماجستير متقدم في إدارة المعلومات الآمنة

التوزيع العام للخطة الدراسية

| الدورة | المادة | الطريقة | عدد الساعات |
|---|---|---|---|
| 1- | تحليلات البيانات في المؤسسة التجارية | إجباري | 150 |
| 1- | إدارة ومعالجة البيانات والمعلومات لعلوم البيانات | إجباري | 150 |
| 1- | أجهزة ومنصات IoT كأساس لعلوم البيانات | إجباري | 150 |
| 1- | العرض البياني لتحليل البيانات | إجباري | 150 |
| 1- | أدوات علوم البيانات | إجباري | 150 |
| 1- | استخراج البيانات. الاختيار والمعالجة والتحويل | إجباري | 150 |
| 1- | الندرة على التنبؤ وتحليل الظواهر العشوائية | إجباري | 150 |
| 1- | تصميم وتطوير الأنظمة الذكية | إجباري | 150 |
| 1- | معماريات وأنظمة للاستخدام المكثف للبيانات | إجباري | 150 |
| 1- | التطبيق العملي لعلوم البيانات في قطاعات النشاط التجاري | إجباري | 150 |

| الدورة | المادة | الطريقة | عدد الساعات |
|---|---|---|---|
| 2- | الذكاء السيبراني والأمن السيبراني | إجباري | 150 |
| 2- | أمن المضيف | إجباري | 150 |
| 2- | أمان الشبكة (المحيطية) | إجباري | 150 |
| 2- | أمان الهاتف الذكي | إجباري | 150 |
| 2- | أمن إنترنت الأشياء IoT | إجباري | 150 |
| 2- | القرصنة الأخلاقية | إجباري | 150 |
| 2- | الهندسة العكسية | إجباري | 150 |
| 2- | التنمية الآمنة | إجباري | 150 |
| 2- | التحليل الجنائي | إجباري | 150 |
| 2- | التحديات الحالية والمستقبلية في أمن الكمبيوتر | إجباري | 150 |

أ. د./ Tere Guevara Navarro

رئيس الجامعة

الجامعة التكنولوجية

*تصديق لاهاي أبوستيل. في حالة طلب الطالب الحصول على درجته العلمية الورقية وبتصديق لاهاي أبوستيل، ستتخذ مؤسسة TECH EDUCATION الخطوات المناسبة لكي يحصل عليها بتكلفة إضافية.

الجامعة التيكنولوجية

## ماجستير متقدم

## إدارة المعلومات الآمنة

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **سنتين**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- عدد الساعات المخصصة للدراسة: **16 ساعات أسبوعيًا**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

# ماجستير متقدم

# إدارة المعلومات الآمنة


tech الجامعة التيكنولوجية