ماجستير خاص
MBA إدارة الأمن السيبراني
(CISO، مدير أمن المعلومات)

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

ماجستير خاص
MBA إدارة الأمن السيبراني
(CISO، مدير أمن المعلومات)

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **12 شهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

رابط الدخول إلى الموقع الإلكتروني: www.techtitute.com/ae/information-technology/professional-master-degree/master-cybersecurity-management-ciso-chief-information-security-officer

الفهرس

01

المقدمة

مع تقدم التكنولوجيا، تتقدم التهديدات أيضاً، وتتقن أساليبها الهجومية. بعبارة أخرى، تتزايد إمكانيات وسبل تحقيق مجرمي الإنترنت لأهدافهم. في هذا السياق تقدم جامعة TECH مؤهلًا يستطيع من خلاله المحترفون اللحاق بالركب، ويتعلمون بطريقة شاملة كيفية حماية وتأمين البيئات الرقمية المختلفة. كل هذا، من خلال منهجية ثورية هي إعادة التعلم؛ وبصيغة مريحة ومتاحة بالكامل عبر الإنترنت، مما سيتيح للخريج اكتساب المهارات والقدرات دون توقيت محدد مسبقًا. بالتالي، عند الانتهاء من هذه الشهادة، سيحصل المحترف على المهارات والكفاءات اللازمة لممارسة منصب كبير مسؤولي أمن المعلومات بكفاءة، وهو منصب إداري رفيع المستوى مرموق للغاية مع آفاق كبيرة للنمو والتوسع.

مع تقدم التكنولوجيا والاتصال، يتزايد عدد وشكل التهديدات المحتملة. لذلك، من الضروري أن يقوم كبار مسؤولي أمن المعلومات المستقبليين بتحديث معارفهم لتقديم حلول أكثر تكيفًا مع خصوصيات الشركة"

لا يخفى على أحد أننا في خضم عصر المعلومات والاتصالات، حيث أننا جميعًا متصلون ببعضنا البعض، سواء في المنزل أو في بيئات الشركات. بالتالي، يمكننا الوصول إلى العديد من المعلومات بنقرة واحدة من خلال بحث واحد في أي من المحركات المتاحة لنا، سواء من هاتف ذكي أو كمبيوتر شخصي أو كمبيوتر العمل.

تمامًا كما تتقدم التكنولوجيا بالنسبة للمواطن العادي والموظف، كذلك تتطور تقنيات التهديدات والهجوم. كلما زادت الوظائف الجديدة وكلما زاد عدد الوظائف الجديدة وكلما زاد التواصل، زادت مساحة الهجوم. في ظل هذا السياق المثير للقلق، تطلق جامعة TECH هذا MBA إدارة الأمن السيبراني (CISO، مدير أمن المعلومات)، والذي تم تطويره من قبل فريق عمل من ذوي الخبرات المهنية المختلفة والمتخصصة في قطاعات مختلفة يجمع بين الخبرة المهنية الدولية في القطاع الخاص في مجال البحث والتطوير والابتكار والخبرة الواسعة في مجال التدريس.

كما توفر درجة الماجستير هذه للطلاب دروساً إضافية ممتازة وكاملة يقوم بتدريسها متخصص في الذكاء والأمن الالكتروني والتقنيات التخريبية ذو مكانة دولية مرموقة. سيكون هذا المحتوى المبتكر متاحًا في شكل 10 صفوف رئيسية متقدمة حصرية ستمكن الخريجين من تحديث معرفتهم بالأمن الإلكتروني وإدارة الأقسام المسؤولة عن هذه المهام في أهم الشركات في قطاع التكنولوجيا.

يشمل البرنامج مختلف الموضوعات الأساسية في مجال الأمن الإلكتروني، والتي تم اختيارها بعناية لتغطي بدقة طيفاً واسعاً من التقنيات القابلة للتطبيق في مجالات العمل المختلفة. لكنه سيتعامل أيضًا مع فرع آخر من الموضوعات التي عادة ما تكون نادرة في الفهرس الأكاديمي للمؤسسات الأخرى والتي ستغذي بعمق السيرة الذاتية للمهني. بهذه الطريقة، وبفضل المعرفة المستعرضة التي يقدمها هذا البرنامج، سيكتسب الخريج المهارات اللازمة للعمل كمدير في مجال الأمن الإلكتروني (كبير مسؤولي أمن المعلومات)، وبالتالي زيادة آفاق النمو الشخصي والمهني.

يحتوي **ماجستير خاص في MBA إدارة الأمن السيبراني (CISO، مدير أمن المعلومات)** على البرنامج التعليمي الأكثر اكتمالاً وحداثة في السوق. أبرز خصائصها هي:

- تطوير حالات عملية مقدمة من خبراء الأمن السيبراني
- محتوياتها البيانية والتخطيطية والعملية البارزة التي يتم تصورها بها تجمع المعلومات العلمية والرعاية العملي حول تلك التخصصات الأساسية للممارسة المهنية
- التمارين العملية حيث يمكن إجراء عملية التقييم الذاتي لتحسين التعلم
- تركيزها على المنهجيات المبتكرة
- كل هذا سيتم استكماله بدروس نظرية وأسئلة للخبراء ومنتديات مناقشة حول القضايا المثيرة للجدل وأعمال التفكير الفردية
- توفر المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

استعد مع أفضل المحترفين! استفد من 10 صفوف رئيسية متقدمة يقدمها محاضر مشهور عالمياً"

تميّز في هذا القطاع المزدهر وكن خبيراً في مجال الأمن الإلكتروني مع MBA من جامعة TECH. إنه الأكثر اكتمالا في السوق"

تتطور الطرق التي يتبادل بها الناس المعلومات بسرعة. هذا يتطلب من المتخصصين أشكال جديدة من الحماية الإلكترونية.

برنامج 100% عبر الإنترنت يركز على الممارسة التي ستضع الأسس لنموك المهني.

البرنامج يضم في طاقم اتدريس محترفين في القطاع الذين يجلبون لهذا التدريب خبراتهم في عملهم، بالإضافة إلى متخصصين معترف بهم من المجتمعات الرائدة والجامعات المرموقة.

سيتيح محتوى البرنامج المتعدد الوسائط، والذي صيغ بأحدث التقنيات التعليمية، للمهني التعلم السياقي والموقعي، أي في بيئة محاكاة توفر تدريبا غامرا مبرمجا للتدريب في حالات حقيقية.

يركز تصميم هذا البرنامج على التعلّم القائم على حل المشكلات، والذي يجب على المهني من خلاله محاولة حل مختلف مواقف الممارسة المهنية التي تنشأ على مدار العام الدراسى. للقيام بذلك، سيحصل على مساعدة من نظام فيديو تفاعلي مبتكر من قبل خبراء مشهورين.

02

الأهداف

إدراكًا منها لأهمية الأمن السيبراني للشركات والأفراد، طورت جامعة TECH هذا MBA الذي يهدف إلى تعزيز وتحديث معرفة المتخصصين في الكشف عن الجرائم الإلكترونية وحمايتها والوقاية منها. بهذه الطريقة، سيصبح خريج المستقبل لاعبًا رئيسيًا في رعاية البيانات والمعلومات، مما يقلل من إمكانية استفادة المجرمين من الاختراقات الأمنية الحالية. الكفاءة المهنية التي سيتمكن المهني من اكتسابها في تيك، في غضون 12 شهرًا فقط.

هذه فرصة فريدة من نوعها لتحقيق أحلامك وأهدافك
وأن تصبح خبيراً في مجال الأمن الإلكتروني"

الأهداف العامة

- تحليل دور المحلل في الأمن السيبراني
- تعميق فهم الهندسة الاجتماعية وأساليبها
- فحص منهجيات OSINT و HUMINT و OWASP و PTEC. OSSTMM و OWISAM
- إجراء تحليل للمخاطر ومعرفة مقاييس المخاطر
- تحديد الاستخدام الصحيح لإخفاء الهوية واستخدام الشبكات مثل TORو I2P و Freenet
- توليد المعرفة المتخصصة لإجراء التدقيق الأمني
- تطوير سياسات الاستخدام المناسبة
- فحص أنظمة الكشف والوقاية من أهم التهديدات
- تقييم أنظمة الكشف الجديدة عن التهديدات، وكذلك تطورها فيما يتعلق بالحلول الأكثرتقليدية
- تحليل منصات المحمول الرئيسية الحالية وخصائصها واستخدامها
- تحديد وتحليل وتقييم المخاطر الأمنية لأجزاء مشروع إنترنت الأشياء 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 الطب الشرعي
- تقديم تقرير التحليل الجنائي على النحو الواجب
- تحليل الحالة الراهنة والمستقبلية لأمن الحاسوب
- دراسة مخاطر التكنولوجيات الجديدة الناشئة
- تجميع التكنولوجيات المختلفة فيما يتعلق بأمن الحاسوب

الأهداف المحددة

الوحدة 1. الذكاء والأمن السيبراني

- تطوير المنهجيات المستخدمة في مجال الأمن الإلكترونى
- دراسة دورة الاستخبارات وإثبات تطبيقها في مجال الاستخبارات الإلكترونية
- تحديد دور المحلل الاستخباري ومعوقات نشاط الاخلاء
- تحليل منهجيات استخبارات المصادر المفتوحة و الأمن في الشبكات اللاسلكية و دليل منهجية اختبار الأمان مفتوح المصدر و منهجية اختبار الاختراق وفتح مشروع أمان تطبيقات الويب
- إنشاء الأدوات الأكثر شيوعًا لإنتاج المعلومات الاستخبارية
- إنشاء الأدوات الأكثر شيوعًا لإنتاج المعلومات الاستخبارية
- تحديد خيارات إخفاء الهوية واستخدام الشبكات مثل تور (شبكة TOR) و مشروع الإنترنت المخفية FreeNet
- تفاصيل لوائح الأمن الإلكتروني الحالية

الوحدة 2. أمن host

- تحديد سياسات النسخ الاحتياطي للبيانات الشخصية والمهنية
- تقييم الأدوات المختلفة لتقديم حلول لمشاكل أمنية محددة
- إنشاء آليات للحصول على نظام محدث
- تحليل المعدات للكشف عن المتسللين
- تحديد قواعد الوصول إلى النظام
- فحص وتصنيف رسائل البريد الإلكتروني لمنع الاحتيال
- وضع قوائم بالبرامجيات المسموح بها

الوحدة 3. أمان الشبكة (المحيط)

- تحليل هياكل الشبكة الحالية لتحديد المحيط الذي يجب علينا حمايته
- تطوير الإعدادات الأساسية لجدار الحماية firewall ولينيكس Linux للتخفيف من الهجمات الأكثر شيوعا
- تجميع الحلول الأكثر استخدامًا مثل Snort و Meerkat، بالإضافة إلى إعداداتها
- فحص الطبقات الإضافية المختلفة التي يوفرها firewalls من جدران الحماية ووظائف الشبكة في بيئات Cloud.
- تحديد أدوات حماية الشبكة واشرح سبب أهميتها للدفاع متعدد الطبقات

الوحدة 4. أمن الهواتف الذكية smartphones

- فحص نواقل الهجوم المختلفة لتجنب أن تصبح هدفًا سهلاً
- تحديد الهجمات الرئيسية وأنواع البرمجيات الخبيثة التي يتعرض لها مستخدمو الأجهزة المحمولة
- تحليل أحدث الأجهزة لتأسيس أمان أكبر في الاعداد
- تحديد الخطوات الرئيسية لإجراء اختبار الاختراق على كل من أنظمة iOS وأنظمة Android
- تطوير المعرفة المتخصصة حول أدوات الحماية والأمن المختلفة
- تأسيس ممارسات جيدة في البرمجة الموجهة للأجهزة المحمولة

الوحدة 5. الأمن في إنترنت الأشياء IoT

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

الوحدة 6. القرصنة Hacking الأخلاقية

- فحص طرق استخبارات المصادر المفتوحة
- جمع المعلومات المتاحة في وسائط الإعلام العامة
- فحص الشبكات للحصول على معلومات الوضع النشط
- تطوير معامل الاختبار
- تحليل الأدوات لأداء pentesting
- فهرسة وتقييم مواطن الضعف المختلفة في النظام
- تحديد منهجيات القرصنة المختلفة

الوحدة 7. الهندسة العكسية

- تحليل مراحل جامع البيانات
- فحص بنية المعالج x86 وبنية معالج معمارية آرم
- تحديد الأنواع المختلفة من التحليل
- تطبيق وضع الحماية في بيئات مختلفة
- تطوير تقنيات تحليل البرامج الضارة المختلفة
- إنشاء أدوات تهدف إلى تحليل البرمجيات الخبيثة

الوحدة 8. التطوير الآمن

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

الوحدة 9. التحليل الجنائي

- التعرف على العناصر المختلفة التي تضع دليل على الجريمة
- توليد المعرفة المتخصصة للحصول على البيانات من وسائط مختلفة قبل فقدانها
- استعادة البيانات التي تم حذفها عن قصد
- تحليل سجلات النظام والسجلات
- تحديد كيفية تكرار البيانات حتى لا يتم تغيير النسخ الأصلية
- إثبات الأدلة على أنها متسقة
- إنشاء تقرير قوي وبدون ثغرات
- عرض النتائج بشكل متماسك
- تحديد كيفية الدفاع عن التقرير أمام السلطة المختصة
- وضع استراتيجيات لجعل العمل عن بعد آمنًا

الوحدة 10. التحديات الحالية والمستقبلية في أمن الحاسوب

- دراسة استخدام العملات الرقمية وتأثيرها على الاقتصاد والأمن
- تحليل حالة المستخدمين ودرجة الأمية الرقمية
- تحديد نطاق استخدام سلسلة الكتل 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
- وضع استراتيجيات لجعل العمل عن بعد آمنًا

الوحدة 11. القيادة والأخلاق والمسؤولية الاجتماعية للشركة

- تحليل تأثير العولمة على حوكمة الشركات وإدارة الشركات
- تقييم أهمية القيادة الفعالة في إدارة ونجاح الشركات
- تحديد استراتيجيات الإدارة متعددة الثقافات وأهميتها في بيئات الأعمال المتنوعة
- تطوير المهارات القيادية وفهم التحديات الحالية التي تواجه القادة
- تحديد مبادئ وممارسات أخلاقيات العمل وتطبيقها في عملية اتخاذ القرارات المؤسسية
- هيكلة استراتيجيات تنفيذ وتحسين الاستدامة والمسؤولية الاجتماعية للشركات

الوحدة 12. قيادة الأفراد وإدارة المواهب

- تحديد العلاقة بين التوجه الاستراتيجي وإدارة الموارد البشرية
- تعميق المهارات اللازمة لإدارة الموارد البشرية الفعالة القائمة على الكفاءة
- تعميق منهجيات تقييم الأداء وإدارة الأداء
- دمج ابتكارات إدارة المواهب وأثرها على الاحتفاظ بالموظفين وولائهم
- تطوير استراتيجيات لتحفيز وتطوير فرق العمل عالية الأداء
- اقتراح حلول فعالة لإدارة التغيير وحل النزاعات في المؤسسات

الوحدة 13. الإدارة الاقتصادية والمالية

- تحليل بيئة الاقتصاد الكلي وتأثيرها على النظام المالي الوطني والدولي
- تحديد نظم المعلومات وذكاء الأعمال لاتخاذ القرارات المالية
- التفريق بين القرارات المالية الرئيسية وإدارة المخاطر في الإدارة المالية
- تقييم استراتيجيات التخطيط المالي وزيادة تمويل الأعمال التجارية

الوحدة 14. الإدارة التجارية والتسويق الاستراتيجي

- هيكلة الإطار المفاهيمي وأهمية إدارة الأعمال في الشركات
- الخوض في العناصر والأنشطة الرئيسية للتسويق وتأثيرها على المؤسسة
- تحديد مراحل عملية التخطيط التسويقي الاستراتيجي
- تقييم استراتيجيات تحسين الإعلام المؤسسي وسمعة الرقمية للشركة

الوحدة 15. Management الاداري

- تحديد مفهوم الإدارة العامة وصلتها بإدارة الأعمال
- تقييم أدوار ومسؤوليات المدير في الثقافة المؤسسية
- تحليل أهمية إدارة العمليات وإدارة الجودة في سلسلة القيمة
- تطوير مهارات الإعلام بين الأشخاص ومهارات التحدث أمام الجمهور لتدريب المتحدثين الرسميين

برنامج فريد ومثالي إذا كنت تتطلع
إلى زيادة معرفتك بالأمن الإلكتروني"

03

الكفاءات

بعد الانتهاء من عملية تقييم درجة الماجستير هذه، سيكون المحترف قد اكتسب سلسلة من المعارف والأدوات والكفاءات التي ستمكنه من العمل في هذا القطاع مع ضمانات أكبر للنجاح. وبهذه الطريقة، لن يصبح الطالب خبيرًا في الأمن الإلكتروني فحسب، بل سيساهم أيضًا بشكل إيجابي في الحد من الجرائم الإلكترونية من خلال صياغة شبكة أكثر أمانًا وقوة للجميع. الوصول إلى مناصب إدارية عليا لمدير أمن المعلومات.

يتطلب قطاع الأمن السيبراني تحديثًا مستمرًا للمعرفة. مع مثل هذه البرامج، يحقق المحترف ذلك بسرعة وفعالية"

الكفاءات العامة

- معرفة المنهجيات المستخدمة في مجال الأمن السيبراني
- معرفة كيفية تقييم كل نوع من أنواع التهديد لتقديم الحل الأمثل في كل حالة
- القدرة على خلق حلول ذكية كاملة لميكنة السلوكيات في حالة وقوع حوادث
- كيفية تقييم المخاطر المرتبطة بنقاط الضعف خارج الشركة وداخلها على حد سواء
- التعرف على تطور وتأثير إنترنت الأشياء بمرور الوقت
- القدرة على إظهار ضعف نظام، ومهاجمته لأغراض وقائية وحل المشكلات المذكورة
- كيفية تطبيق صندوق الحماية في بيئات مختلفة
- التعرف على الإرشادات التي يجب على المطور الجيد اتباعها من أجل الامتثال للأمان المطلوب

سيؤدي تحسين مهاراتك في خدمة الجميع
إلى تعزيز مسيرتك المهنية والشخصية"

الكفاءات المحددة

- التعرف على كيفية تنفيذ عمليات الأمن الدفاعية
- امتلاك تصور عميق ومتخصص لأمن الحاسوب
- امتلاك معرفة متخصصة في مجال الأمن الإلكتروني والاستخبارات الإلكترونية
- فهم أهمية ابتكار دفاع متعدد الطبقات، والمعروف أيضًا باسم "Defense in Depth"، والذي يغطي جميع جوانب شبكة الشركة حيث يمكن أيضًا استخدام بعض المفاهيم والأنظمة التي سنراها وتطبيقها في البيئة المحلية
- التعرف على كيفية تطبيق عمليات الأمان على الهواتف الذكية والأجهزة المحمولة
- التعرف على وسائل تنفيذ مايسمى Hacking الأخلاقي وحماية الشركة من أي هجوم إلكتروني
- القدرة على التحقيق في حادث الأمن السيبراني
- التعرف على تقنيات الهجوم والدفاع المختلفة الموجودة
- تحليل دور المحلل في الأمن السيبراني
- فهم كيفية عمل الهندسة الاجتماعية وأساليبها

04

هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

تم تطوير MBA إدارة الأمن الإلكتروني (CISO، مدير أمن المعلومات) من قبل فريق من الأشخاص ذوي الخبرات المهنية المختلفة والمتخصصة في قطاعات مختلفة، حيث يجمع بين الخبرة المهنية الدولية في القطاع الخاص في مجال البحث والتطوير والابتكار والخبرة الواسعة في التدريس. لذلك، فهم ليسوا محدثين فقط مع كل من التقنيات، ولكن لديهم أيضًا منظورًا حول الاحتياجات المستقبلية للقطاع ويقدمونها بطريقة تعليمية. وبالتالي، فإن المهني مطمئن إلى التعلم من الأفضل في القطاع، مع ضمان الحصول على أحدث المعارف.

خلال MBA سيرافقك عدد من الخبراء المحترفين
الذين سيجعلون تجربتك التعليمية فريدة من نوعها"

المديرة الدولية المستضافة

الدكتور Frederic Lemieux معروف عالميًا كخبير مبتكر وقائد ملهم في مجالات الاستخبارات والأمن القومي والأمن الداخلي والأمن السيبراني والتقنيات التخريبية. الاستخبارات والأمن القومي والأمن الداخلي والأمن الإلكترونى و التقنيات التخريبية. كما أن تفانيه المستمر ومساهماته ذات الصلة في البحث والتعليم يضعه كشخصية رئيسية فى تعزيز الأمنووفهم التقنيات فى الوضع الحالى. خلال مسيرته المهنية، قام خلال مسيرته المهنية بوضع تصورات لبرامج أكاديمية متطورة وإدارتها في عدد من المؤسسات الشهيرة، بما في ذلك جامعة Montreal وجامعة George Washington وجامعة Georgetown.

طوال خلفيته الواسعة، نشر العديد من الكتب ذات الصلة للغاية، وجميعها تتعلقبالاستخبارات الجنائية والعمل السياسى والتهديدات الإلكترونية و الأمن الدولى. بالإضافة إلى ذلك، ساهم بشكل كبير في مجالالأمن الإلكترونىمن خلال نشر العديد من المقالات في المجلات الأكاديمية، التي تتناول مكافحة الجريمة أثناء الكوارث الكبرى ومكافحة الإرهاب ووكالات الاستخبارات، وتعاون الشرطة. بالإضافة إلى ذلك، كان عضوًا في اللجنة ومتحدثًا رئيسيًا في العديد من المؤتمرات الوطنية والدولية، مما جعله مرجعًا في المجال الأكاديمي والمهني.

شغل الدكتور Doctor Lemieux أدوارًا تحريرية وتقييمية في مختلف المؤسسات الأكاديمية والخاصة والحكومية، مما يعكس تأثيره والتزامه بالتميز في مجال تخصصه. وبهذه الطريقة، قادته مسيرته الأكاديمية المرموقة إلى العمل كأستاذ ممارس ومدير هيئة التدريس لبرامج جدول الإنتاج الرئيسيفي الذكاء التطبيقي وإدارة مخاطر الأمن الإلكترونى وإدارة التكنولوجيا و إدارة تكنولوجيا المعلومات فى جامعة Georgetown.

د. Lemieux, Frederic

- مدير برنامج الماجستير في Cybersecurity Risk Management في Georgetown، واشنطن، الولايات المتحدة الأمريكية
- مدير برنامج الماجستير في Technology Management في جامعة Georgetown
- مدير برنامج الماجستير في Applied Intelligence بجامعة Georgetown
- أستاذ التدريب العملي في جامعة Georgetown
- دكتوراه في علم الجريمة من la School of Criminology جامعة Montreal
- ليسانس في علم الاجتماع وحاصل على درجة Minor Degree في علم النفس من جامعة Laval
- عضو في: New Program Roundtable Committee، جامعة Georgetown

بفضل TECH ستتمكن من التعلم
مع أفضل المحترفين في العالم"

المديرة الدولية المستضافة

بخبرة تزيد عن 20 عاماً في تصميم وقيادة فرق عالمية لاستقطاب المواهب، Jennifer Dove هي خبيرة في التوظيف و استراتيجية التكنولوجيا. وقد شغلت طوال حياتها المهنية مناصب رفيعة في العديد من المؤسسات التكنولوجية في العديد من الشركات المدرجة على قائمة فورتشن 50، بما في ذلك NBCUniversal و Comcast. وقد مكّنه سجله الحافل من التفوق في بيئات تنافسية وعالية النمو.

بصفتها نائبة رئيس قسم استقطاب المواهب في Mastercard، تشرف على استراتيجية استقطاب المواهب وتنفيذها، وتتعاون مع قادة الأعمال ومسؤولي الموارد البشرية لتحقيق أهداف التوظيف التشغيلية والاستراتيجية. هي تهدف على وجه الخصوص إلى إنشاء فرق عمل متنوعة وشاملة وذات أداء عالٍ تدفع الابتكار والنمو في منتجات الشركة وخدماتها. كما أنها خبيرة في استخدام الأدوات اللازمة لجذب أفضل المهنيين من جميع أنحاء العالم والاحتفاظ بهم. كما تتولى مسؤولية تعزيز علامة صاحب العمل التجارية والقيمة التي تقدمها Mastercard من خلال المنشورات والفعاليات ووسائل التواصل الاجتماعي.

أثبتت Jennifer Dove التزامها بالتطوير المهني المستمر، حيث شاركت بنشاط في شبكات المتخصصين في مجال الموارد البشرية وساهمت في توظيف العديد من الموظفين في شركات مختلفة. بعد حصولها على درجة البكالوريوس في الاتصال التنظيمي من جامعة ميامي، شغلت مناصب عليا في مجال التوظيف في شركات في مجالات متنوعة.

من جهة أخرى، قد اشتهرت بقدرتها على قيادة التحولات التنظيمية، ودمج التكنولوجيا في عمليات التوظيف، وتطوير برامج القيادة التي تُعد المؤسسات للتحديات المقبلة. قد نجحت أيضاً في تنفيذ برامج العافية المهنية التي زادت بشكل كبير من رضا الموظفين والاحتفاظ بهم.

أ. Dove، Jennifer

- نائب الرئيس في استقطاب المواهب في Mastercard، نيويورك، الولايات المتحدة الأمريكية
- مديرة استقطاب المواهب، NBCUniversal، نيويورك، الولايات المتحدة الأمريكية
- رئيسة قسم التوظيف Comcast
- رئيسة قسم التوظيف في شركة Rite Hire Advisory
- نائب الرئيس التنفيذي، قسم المبيعات في شركة Ardor NY Real Estate
- مديرة التوظيف في شركة Valerie August وشركاه
- مديرة تنفيذية للحسابات في شركة BNC
- مديرة تنفيذية للحسابات في Vault
- خريجة في الإعلام المؤسسي من جامعة ميامي

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

المدير الدولي المستضاف

رائد تقني مع عقود من الخبرة في مجال التكنولوجيا في كبرى شركات التكنولوجيا متعددة الجنسيات، Rick Gauthier طور بشكل بارز في مجال الخدماتالسحابية وتحسين العمليات من البداية إلى النهاية. وقد تم الاعتراف به كقائد ومدير فريق ذو كفاءة عالية، حيث أظهر موهبة طبيعية لضمان مستوى عالٍ من الالتزام بين موظفيه.

فهو يتمتع بموهبة فطرية في الاستراتيجية والابتكار التنفيذي، وتطوير أفكار جديدة ودعم نجاحها ببيانات عالية الجودة. وقد أتاحت له مسيرته المهنية في Amazon إدارة ودمج خدمات تكنولوجيا المعلومات الخاصة بالشركة في الولايات المتحدة. قاد في شركة Microsoft فريقًا مكونًا من 104 أشخاص، وكان مسؤولاً عن توفير البنية التحتية لتكنولوجيا المعلومات على مستوى الشركة ودعم أقسام هندسة المنتجات في جميع أنحاء الشركة.

وقد مكنته هذه الخبرة من البروز كمدير عالي التأثير يتمتع بقدرات ملحوظة على زيادة الكفاءة والإنتاجية ورضا العملاء بشكل عام.

أ. Gauthier، Rick

- مدير تكنولوجيا المعلومات الإقليمي في Amazon، Seattle، الولايات المتحدة الأمريكية
- رئيس قسم البرامج العليا في Amazon
- نائب رئيس شركة Wimmer Solutions
- المدير الأول لخدمات الهندسة الإنتاجية في Microsoft
- شهادة في الأمن السيبراني من Western Governors University
- شهادة تقنية في الغوص التجاري *Commercial Diving* من Divers Institute of Technology
- شهادة في الدراسات البيئية من The Evergreen State College

"اغتنم الفرصة للتعرف على أحدث التطورات في هذا المجال لتطبيقها في ممارستك اليومية"

المدير الدولي المستضاف

Romi Arman هو خبير دولي شهير يتمتع بخبرة تزيد عن عقدين من الزمن في مجال التحول الرقمي, والتسويق، والاستراتيجيات و الاستشارات. وطوال مسيرته المهنية الطويلة، قام بالعديد من المخاطر، وهو مدافع دائم عن الابتكار و التغيير في بيئة الأعمال. وبفضل هذه الخبرة، عمل مع رؤساء تنفيذيين وشركات في جميع أنحاء العالم، ودفعهم إلى الابتعاد عن نماذج الأعمال التقليدية. وهكذا، قد ساعد شركات مثل Shell للطاقة على أن تصبح شركات رائدة حقيقية في السوق، مع التركيز على عملائها و العالم الرقمي.

إن الاستراتيجيات التي صممها Arman لها تأثير كامن، حيث مكنت العديد من الشركات من تحسين تجارب المستهلكين، والموظفين و المساهمين على حد سواء. نجاح هذا الخبير يمكن قياسه كمياً من خلال مقاييس ملموسة مثل CSAT، و مشاركة الموظفين في المؤسسات التي عمل فيها ونمو المؤشر المالي للأرباح قبل خصم الفوائد والضرائب والاستهلاك والإطفاء في كل منها.

كما قام أيضاً برعاية وقيادة فرق عالية الأداء حصلت على جوائز تقديراً لإمكاناتها التحويلية.. مع شركة Shell، بالتحديد، شرع المدير التنفيذي في التغلب على ثلاثة تحديات: تلبية متطلبات من أجل ازالة الكربون المعقدة للعملاء، ودعم"إزالة الكربون الفعالة من حيث التكلفة" و إصلاح مشهد مجزأ للبيانات, والرقمية والتكنولوجيا. وبالتالي، فقد أظهرت جهودهم أنه من أجل تحقيق النجاح المستدام، من الضروري البدء من احتياجات المستهلكين وإرساء أسس التحول في العمليات والبيانات والتكنولوجيا والثقافة.

من ناحية أخرى، يتميز المدير التنفيذي بإتقانه لتطبيقات الذكاء الاصطناعي في مجال الأعمال، وهو موضوع يحمل فيه شهادة الدراسات العليا من كلية لندن للأعمال. وفي الوقت نفسه، اكتسب خبرة متراكمة في مجال إنترنت الأشياء و Salesforce.

أ. Arman، Romi

- مدير التحوّل الرقمي (CDO) في شركة Shell للطاقة، لندن، المملكة المتحدة
- الرئيس العالمي للتجارة الإلكترونية وخدمة العملاء في شركة Shell للطاقة
- مدير الحسابات الرئيسية الوطنية (مصنعي المعدات الأصلية للسيارات والتجزئة) لشركة Shell في كوالالمبور، ماليزيا
- مستشار إداري أول (قطاع الخدمات المالية) لدى شركة Accenture من سنغافورة
- خريج جامعة Leeds
- الدراسات العليا في تطبيقات الذكاء الاصطناعي في مجال الأعمال لكبار التنفيذيين من كلية لندن للأعمال
- شهادة محترف تجربة العملاء CCXP
- دورة التحول الرقمي التنفيذي من IMD

هل ترغب في تحديث معرفتك بأعلى جودة تعليمية؟ تقدم لك جامعة TECH أحدث محتوى في السوق الأكاديمي، صممه خبراء مشهورون دوليًا"

المدير الدولي المستضاف

Manuel Arens هو خبير متمرس في إدارة البيانات وقائد فريق عمل على درجة عالية من الكفاءة. في الواقع، يشغل Arens منصب مدير المشتريات العالمية في قسم البنية التحتية التقنية ومركز البيانات في Google، حيث قضى معظم حياته المهنية. وقد قدمت الشركة، التي يقع مقرها في Mountain View، حلولاً للتحديات التشغيلية التي تواجه عملاق التكنولوجيا، مثل تكامل البيانات الرئيسية، و تحديثات بيانات البائعين وتحديد أولويات بيانات البائعين. وقد قاد عملية تخطيط سلسلة التوريد في مركز البيانات وتقييم مخاطر الموردين، مما أدى إلى تحسينات في العمليات وإدارة سير العمل أدت إلى تحقيق وفورات كبيرة في التكاليف.

مع أكثر من عشر سنوات من العمل في تقديم الحلول الرقمية والقيادة للشركات في مختلف الصناعات، يتمتع بخبرة واسعة في جميع جوانب تقديم الحلول الاستراتيجية، بما في ذلك التسويق، وتحليلات الوسائط، medición و القياس والإسناد. في الواقع، حصلت الشركة على العديد من الجوائز عن عملها، بما في ذلك جائزة الريادة BIM، و جائزة الريادة في البحث، جائزة برنامج توليد العملاء المحتملين للتصدير و جائزة أفضل نموذج مبيعات في أوروبا والشرق الأوسط وأفريقيا.

كما شغل Arens منصب مدير المبيعات في Dublín، أيرلندا. في هذا المنصب، قام ببناء فريق من 4 إلى 14 عضوًا في ثلاث سنوات وقاد فريق المبيعات لتحقيق النتائج والتعاون بشكل جيد مع بعضهم البعض ومع الفرق متعددة الوظائف. كما عمل أيضاً كمحلل أول للصناعة في هامبورغ بألمانيا، حيث قام بإعداد خطوط سير لأكثر من 150 عميلاً باستخدام أدوات داخلية وخارجية لدعم التحليل. تطوير وكتابة تقارير متعمقة لإثبات إتقان الموضوع، بما في ذلك فهم العوامل الاقتصادية الكلية والسياسية/التنظيمية التي تؤثر على تبني التكنولوجيا ونشرها.

وقد قاد أيضاً فرق عمل في شركات مثل Airbus، Eaton، Siemensg، حيث اكتسب خبرة قيّمة في إدارة الحسابات وسلسلة التوريد. وقد اشتهر بشكل خاص بعمله على تجاوز التوقعات باستمرار من خلال بناء علاقات قيّمة مع العملاء و العمل بسلاسة مع الأشخاص على جميع مستويات المؤسسة، بما في ذلك أصحاب المصلحة والإدارة وأعضاء الفريق والعملاء. لقد جعله نهجه القائم على البيانات وقدرته على تطوير حلول مبتكرة وقابلة للتطوير لتحديات الصناعة رائداً بارزاً في مجاله.

أ. Arens, Manuel

- مدير المشتريات العالمية في Google، Mountain View، الولايات المتحدة الأمريكية
- مدير أول، تحليلات وتكنولوجيا B2B، Google، الولايات المتحدة الأمريكية
- مدير مبيعات فيGoogle، أيرلندا
- كبير محللي الصناعة في Google، ألمانيا
- مدير حساب في Google، أيرلندا
- Accounts Payable في إيتون، المملكة المتحدة
- مدير سلسلة التوريد في شركة Airbus، ألمانيا

راهن على جامعة TECH! ستتمكن من الوصول إلى أفضل المواد التعليمية، في طليعة التكنولوجيا والتعليم، والتي ينفذها متخصصون مشهورون دوليًا في هذا المجال"

المدير الدولي المستضاف

Andrea La Sala هو مدير تنفيذي في مجال التسويق كان لمشاريعه معنى مؤثر في بيئة الأزياء. وطوال مسيرته المهنية الناجحة قام بتطوير مجموعة متنوعة من المهام المتعلقة بالمنتجات، والتسويق و الإعلامات. كل هذا مرتبط بعلامات تجارية مرموقة مثل Giorgio Armani, Dolce&Gabbana، Calvin Klein، وغيرها.

وقد ارتبطت نتائج هذا المدير من أعلى المستويات الدولية بقدرته المثبتة على تجميع المعلومات في أطر عمل واضحة وتنفيذ إجراءات ملموسة تتماشى مع أهداف العمل المحددة. بالإضافة إلى ذلك، فهو معروف باستباقيته و قدرته على التكيف مع الإيقاع السريع للعمل. ومع كل هذا، يضيف هذا الخبير وعياً تجارياً قوياً،ورؤية للسوق و شغفاً حقيقياً بالمنتجات.

كمدير عالمي للعلامات التجارية والتسويق في Giorgio Armani، أشرف على استراتيجيات تسويقية مختلفة للملابس و الإكسسوارات. كما ركزت تكتيكاتهم أيضًا في مجال البيع بالتجزئة و احتياجات المستهلكين وسلوكهم. في هذا كان La Sala مسؤولاً أيضاً عن تشكيل تسويق المنتجات في الأسواق المختلفة، حيث عمل كقائد فريق في أقسام التصميم، والإعلامات و المبيعات.

ومن ناحية أخرى، قام في شركات مثل Calvin Klein أو Gruppo Coin، بمشاريع لتعزيز هيكلية، لكلا التطوير و التسويق لـ مجموعات مختلفة. كما كان مسؤولاً عن إنشاء تقويمات فعالة لكل من حملات البيع والشراء. كما كان مسؤولاً عن شروط، وتكاليف، وعمليات و مواعيد تسليم العمليات المختلفة.

وقد جعلت هذه الخبرات من Andrea La Sala أحد أهم والأكثر تأهيل لقيادة الشركات في مجال الأزياء و الرفاهية. قدرة إدارية عالية تمكّن من خلالها بطريقة فعالة من تنفيذ التموضع الإيجابي لـ علامات التجارية المختلفة وإعادة تحديد مؤشرات الأداء الرئيسية (KPIs).

أ. La Sala, Andrea

- المدير العالمي للعلامة التجارية والتسويق العالمي لعلامة Armani Exchange en Giorgio Armani، ميلانو، إيطاليا
- مدير التسويق التجاري في Calvin Klein
- مدير العلامة التجارية في Gruppo Coin
- مدير العلامة التجارية في Dolce&Gabbana
- مدير العلامة التجارية في Sergio Tacchini S.p.A
- محلل السوق في Fastweb
- خريج كلية إدارة الأعمال والاقتصاد في جامعة Piemonte الشرقية

ينتظرك أكثر المتخصصين الدوليين تأهيلاً وخبرة في جامعة TECH ليقدموا لك تعليمًا من الدرجة الأولى ومحدثًا ومبنيًا على أحدث الأدلة العلمية. ما الذي تنتظره بعد؟"

المدير الدولي المستضاف

Mick Gram مرادف للابتكار والتميز في مجال ذكاء الأعمال لى المستوى الدولي. ترتبط مسيرته المهنية الناجحة بمناصب قيادية في شركات متعددة الجنسيات مثل Walmart و Red Bull. كما أنه معروف برؤيته في تحديد التقنيات الناشئة التي لها تأثير دائم على المدى الطويل على بيئة الشركات.

من ناحية أخرى، يُعتبر المدير التنفيذي رائداً في استخدام تقنيات تصور البيانات التي تبسّط المجموعات المعقدة وتجعلها في متناول الجميع وتسهّل عملية اتخاذ القرار. وقد أصبحت هذه المهارة الدعامة الأساسية لملفه المهني، مما جعله رصيدًا مرغوبًا فيه لدى العديد من المنظمات التي كانت ملتزمة بجمع المعلومات و توليد إجراءات ملموسة بناءً عليها.

ومن أبرز مشاريعها في السنوات الأخيرة منصة Walmart Data Cafe، وهي أكبر منصة من نوعها في العالم تعتمد على السحابة لتحليل البيانات الضخمة Big Data. وقد شغل أيضاً منصب مدير ذكاء الأعمال Business Intelligence في شركة Red Bull, حيث غطى مجالات مثل المبيعات والتوزيع والتسويق وعمليات سلسلة التوريد. وقد تم تكريم فريقه مؤخراً لابتكاراته المستمرة في استخدام واجهة برمجة تطبيقات Walmart Luminate API الجديدة الخاصة بالمتسوقين وقنوات التسوق.

أما بالنسبة إلى تعليمه، فقد حصل المدير التنفيذي على العديد من شهادات الماجستير والدراسات العليا في مراكز مرموقة مثل جامعة Berkeley،في الولايات المتحدة و جامعة Copenhague،في الدنمارك. ومن خلال هذا التحديث المستمر، يكون الخبير قد حقق أحدث الكفاءات. وعلى هذا النحو، فقد أصبح يُنظر إليه على أنه قائد مولود للاقتصاد العالمي الجديد،, الذي يتمحور حول السعي وراء البيانات وإمكانياتها اللانهائية.

أ. Gram, Mick

- مدير ذكاء الأعمال Business Intelligence والتحليلات في Red Bull, الولايات المتحدة الأمريكية
- مهندس حلول ذكاء الأعمال Business Intelligence في Walmart Data Cafe
- استشاري مستقل لذكاء الأعمال Business Intelligence وعلوم البيانات Data Science
- مدير ذكاء الأعمال Business Intelligence في Capgemini
- محلل أول في Nordea
- استشاري أول ذكاء الأعمال Bussiness Intelligence في SAS
- التعليم التنفيذي في IA Machine Learningg في UC Berkeley Colleg of Engineering
- Executive MBA في التجارة الإلكترونية في جامعة Copenhague
- اجازة وماجستير في الرياضيات والإحصاء في جامعة Copenhague

"ادرس في أفضل جامعة أونلاين في العالم وفقاً لمجلة فوربس! ستتمكن في MBA هذا من الوصول إلى مكتبة واسعة من موارد الوسائط المتعددة التي طورها أساتذة مشهورون عالمياً"

المدير الدولي المستضاف

Scott Stevenson هو خبير متميز في قطاع التسويق الرقمي Marketing Digital ارتبط لأكثر من 19 عام بواحدة من أقوى الشركات في مجال الترفيه، وهي شركة، Warner Bros. Discovery. في هذا المنصب، لعب دوراً رئيسياً في الإشراف على الخدمات اللوجستية و سير العمل الإبداعي عبر مجموعة متنوعة من المنصات الرقمية، بما في ذلك وسائل الإعلام الاجتماعي والبحث والعرض والوسائط الخطية.

لقد كانت قيادة هذا المدير التنفيذي حاسمة في قيادة استراتيجيات الإنتاج فيالإعلامي المدفوع، مما أدى الى نتائج ملحوظة افضل في معدلات التحويل في شركته. وفي الوقت نفسه، تولى في الوقت نفسه مناصب أخرى، مثل مدير خدمات التسويق ومدير حركة المرور في نفس الشركة متعددة الجنسيات خلال فترة إدارته السابقة.

شارك أيضاً في التوزيع العالمي لألعاب الفيديو و حملات الملكية الرقمية. كما كان مسؤولاً أيضاً عن تقديم الاستراتيجيات التشغيلية المتعلقة بتشكيل ووضع اللمسات الأخيرة على محتوى الصوت والصورةللإعلانات التلفزيونية و المقاطع الدعائية.

بالإضافة إلى ذلك، يحمل الخبير اجازة في الإعلامات السلكية واللاسلكية من جامعة فلوريدا والماجستير في الكتابة الإبداعية من جامعة كاليفورنيا، مما يدل على مهاراته في الإعلام و رواية القصص. الإضافة إلى ذلك، شارك في كلية التطوير المهني بجامعة Harvard في برامج متطورة حول استخدام الذكاء الاصطناعي في الأعمال التجارية. وبالتالي، فإن ملفه المهني هو أحد أكثر الملفات المهنية أهمية في مجال التسويق و الإعلام الرقمي الحالي.

أ. Stevenson, Scott

- مدير التسويق الرقمي في Warner Bros. Discovery، Burbank، الولايات المتحدة
- مدير حركة المرور Warner Bros. Entertainment
- ماجستير في الكتابة الإبداعية من جامعة كاليفورنيا
- إجازة في الإعلامات السلكية واللاسلكية من جامعة فلوريدا.

"حقق أهدافك الأكاديمية والمهنية مع أفضل الخبراء المؤهلين في العالم! سيرشدك أساتذة MBA هذا خلال عملية التعلم بأكملها"

المدير الدولي المستضاف

الدكتور Doctor Eric Nyquist هو خبير في في مجال الرياضة العالمية، بنى مسيرة مهنية رائعة، وقد اشتهر بقيادته الاستراتيجية وقدرته على قيادة التغيير والابتكار في المؤسسات الرياضية بمستوى عالي.

في الواقع، لقد شغل مناصب رفيعة مثل مدير الإعلامات والتأثير في NASCAR، في Estados Unidos ،Florida. مع سنوات عديدة من الخبرة، شغل الدكتورNyquist أيضًا عددًا من المناصب القيادية، بما في ذلك نائب الرئيس الأول للتطوير الاستراتيجي و المدير العام لشؤون الأعمال، حيث أدار أكثر من عشرة تخصصات تتراوح بينالتطوير الاستراتيجي و التسويق الترفيهي.

تركNyquist أيضًا بصمة كبيرة على الامتيازات الرياضية الأكثر أهمية في شيكاغو. وبصفته نائب الرئيس التنفيذي لامتيازات Chicago Bulls و Chicago White Sox فقد أثبت قدرته على قيادةالأعمال الناجحة و الاستراتيجية في عالمالرياضة الاحترافية..

وأخيرًا، بدأ مسيرته المهنية فيمجال الرياضة أثناء عمله في نيويورك كـ محلل استراتيجي رئيسي لدى Roger Goodell في الدوري الوطني لكرة القدم الأمريكية وقبل ذلك كمتدرب قانوني لدى الاتحاد الأمريكي لكرة القدم.

أ. Nyquist, Eric

- مدير التواصل والتأثير في NASCAR، في فلوريدا، الولايات المتحدة الأمريكية
- نائب الرئيس الأول للتطوير الاستراتيجي في NASCAR
- نائب رئيس التخطيط الاستراتيجي في NASCAR
- المدير العام لشؤون الأعمال في NASCAR
- نائب الرئيس التنفيذي، امتيازات Chicago White Sox
- نائب الرئيس التنفيذي، امتيازات Chicago Bulls
- مدير تخطيط الأعمال في الدوري الوطني لكرة القدم الأمريكية
- الشؤون التجارية/متدرب الشؤون التجارية/القانونية في الاتحاد الأمريكي لكرة القدم
- دكتوراه من جامعة شيكاغو
- ماجستير في إدارة الأعمال من كلية بوث لإدارة الأعمال في جامعة شيكاغو
- إجازة في الآداب في الاقتصاد الدولي من كلية Carleton

بفضل هذه الشهادة الجامعية 100%، ستتمكن من الجمع بين دراستك والتزاماتك اليومية، بمساعدة كبار الخبراء الدوليين في مجال اهتمامك. سجل الآن!"

هيكل الإدارة

Fernández Sapena, Sonia

- مدربة أمن الحاسوب والقرصنة الأخلاقية في مركز Getafe الوطني المرجعي للحوسبة والاتصالات بمدريد
- مدربة معتمدة من المجلس الإلكتروني
- مدربة في الشهادات التالية: شركة الصناعات الحصرية العامة المحدودة Ethical Hacking Foundation وشركة الصناعات الحصرية العامة المحدودة سايبروتكنولوجيا المعلومات Security Foundation. مدريد
- مدربة خبيرة معتمدة من قبل التصنيع بمساعدة الحاسوب للشهادات 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)
- متعاونة خارجية كبير ضباط الأمن / مهندس أمني أول (Chief Security Officer/Senior Security Architect. في جامعة las Islas Baleares
- مهندسة حاسوب من جامعة Alcalá de Henares في مدريد
- ماجستير في DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

الأساتذة

أ. Marcos Sbarbaro, Victoria Alicia

- مطورة تطبيقات موبايل أندرويد الأصلية B60. المملكة المتحدة
- محللة برمجة لإدارة وتنسيق وتوثيق البيئة الافتراضية للإنذارات الأمنية
- محللة ومبرمجة تطبيقات جافا لأجهزة الصراف الآلي للعميل
- محترفة تطوير Software للتحقق من صحة توقيع العميل وتطبيق إدارة المستندات
- تقنية أنظمة لترحيل المعدات وإدارة وصيانة وتدريب أجهزة المساعد الرقمي الشخصي المحمولة
- مهندسة تقنية في أنظمة الكمبيوتر من جامعة Oberta في كاتالونيا
- ماجستير في أمن الكمبيوتر والقرصنة الأخلاقية الرسمية من EC- Council و CompTIA من قبل المدرسة المهنية للتكنولوجيات الجديدة CICE

أ. Redondo, Jesús Serrano

- مطور ويب وفني الأمن السيبراني
- مطور ويب في Roams،Palencia
- مطور FrontEnd في تليفونيكا، مدريد
- مطور FrontEnd في أفضل شركة استشارات احترافية Best Pro Consulting، مدريد
- مُركِّب معدات وخدمات الاتصالات في Grupo Zener، Castilla،León
- عامل تركيب معدات وخدمات الاتصالات السلكية واللاسلكية في شركة Lican Comunicaciones SL, Castilla y León
- شهادة في أمن معلومات الحاسوب من المركز المرجعي الوطني لتطوير الحاسوب والاتصالات Getafe، مدريد
- فني عالي في الاتصالات وأنظمة الحاسوب من مؤسسات التعليم العالي IES Trinidad Arroyo، Palencia
- فني عالي في التركيبات الكهروتقنية ناقل الحركة اليدوي والجهد المنخفض من مؤسسات التعليم العالى IES Trinidad Arroyo، Palencia
- تدريب في الهندسة العكسية والاختزال والتشفير من أكاديمية Hacker Incibe

أ. Catalá Barba, José Francisco

- تقني إلكترونيات خبير في الأمن السيبراني
- مطور تطبيقات الأجهزة المحمولة
- تقني إلكترونيات في القيادة المتوسطة بوزارة الدفاع الإسبانية
- تقني إلكترونيات في Factoría Ford Sita في Valencia

أ. Peralta Alonso, Jon

- مستشار أول لحماية البيانات والأمن السيبراني في Altia
- محامية/مستشارة قانونية في شركة Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- مستشار قانوني/متدرب في المكتب المهني: Óscar Padura
- إجازة في القانون من جامعة Pública del País Vasco
- ماجستير في حماية البيانات من مدرسة نظام المعلومات التنفيذي Innovative School
- ماجستير في القانون من جامعة Pública del País Vasco
- ماجستير في ممارسة الإجراءات المدنية من جامعة Isabel 1 الدولية de Castilla
- أستاذ محاضر في درجة الماجستير في قانون حماية البيانات الشخصية والأمن الإلكتروني وتكنولوجيا المعلومات والاتصالات أ Jiménez Ramos, Álvaro

أ. Jiménez Ramos, Álvaro

- محلل الأمن السيبراني
- 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.
- إجازة في هندسة الاتصالات عن بعد من جامعة Politécnica بمدريد
- ماجستير في الأمن السيبراني والقرصنة الأخلاقية من المدرسة المهنية للتقنيات الجديدة CICE
- دورة عليا في الأمن السيبراني من قبل Deusto Formación

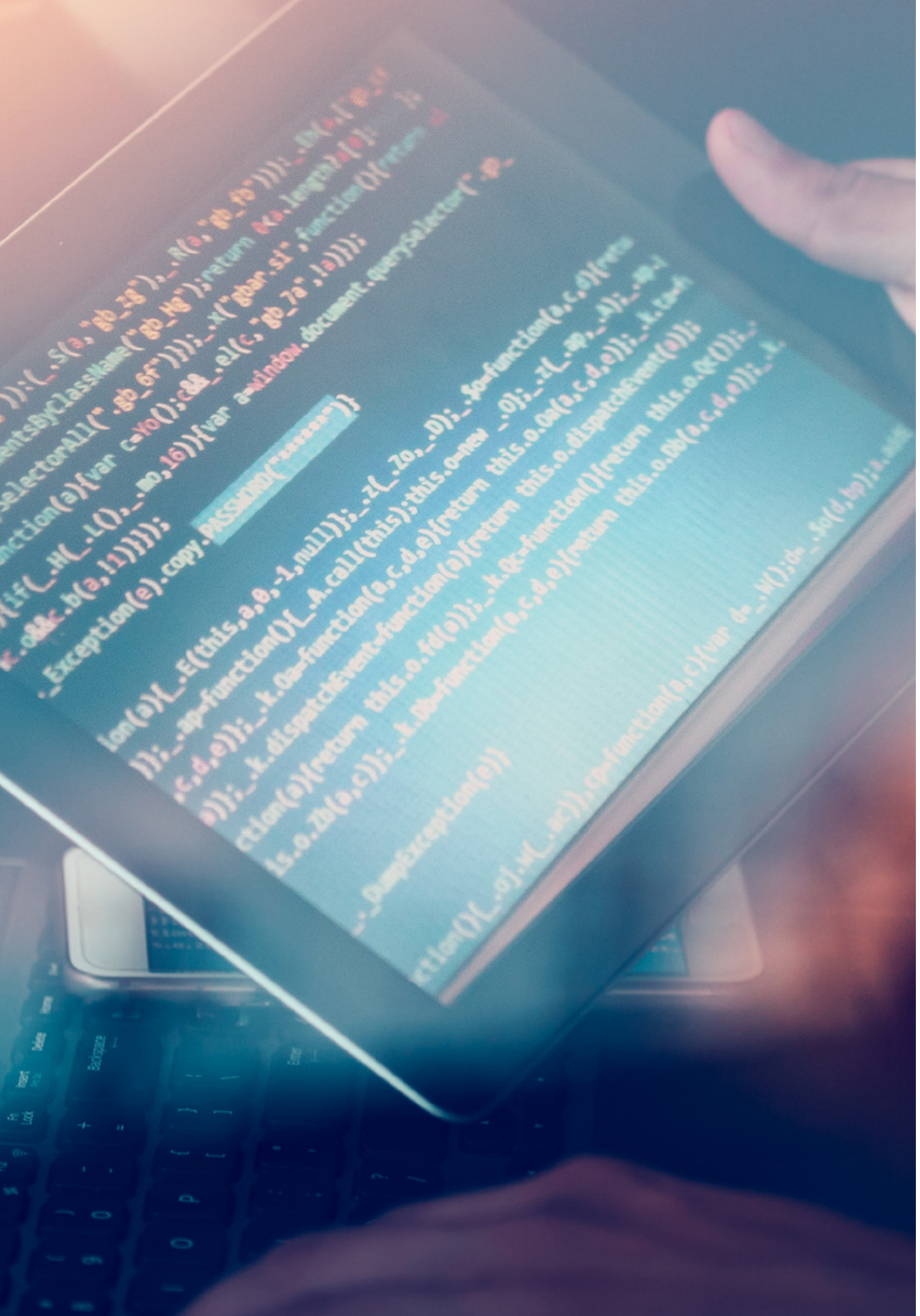
اغتنم الفرصة للتعرف على أحدث التطورات في هذا الشأن لتطبيقها على ممارستك اليومية"

05

الهيكل والمحتوى

تم تصميم المنهج الدراسي على أساس الفعالية التعليمية، واختيار المحتويات بعناية لتقديم محاضرة دراسية كاملة، تشمل جميع مجالات الدراسة الضرورية لتحقيق المعرفة الحقيقية للموضوع. مع آخر التحديثات وجوانب القطاع. هكذا تم وضع منهج دراسي تقدم وحداته الدراسية منظورًا واسعًا للإدارة التقنية لعلوم البيانات في الشركة. من الوحدة الأولى، سيرى الطالب أن معرفته قد توسعت، مما سيمكنه من التطور مهنيًا، مع العلم أنه يحظى أيضًا بدعم فريق من الخبراء.

تم تجميع جميع الموضوعات ومجالات المعرفة في منهج دراسي كامل ومحدث، لنقل الطالب إلى أعلى مستوى نظري وعملي"



الوحدة 1. الذكاء والأمن السيبراني

1.1. الذكاء السيبراني
1.1.1. الذكاء السيبراني
1.1.1.1. الذكاء
1.1.1.1.1. دورة ذكاء
2.1.1.1. الذكاء السيبراني
3.1.1.1. الذكاء والأمن السيبراني
2.1.1. محلل الذكاء
1.2.1.1. دور المحلل الاستخباراتي
2.2.1.1. تحيز محلل الاستخبارات في النشاط التقييمي
2.1. الأمن السيبراني
1.2.1. طبقات الأمان
2.2.1. التعرف على التهديدات السيبراني
1.2.2.1. التهديدات الخارجية
2.2.2.1. التهديدات الداخلية
3.2.1. الإجراءات العكسية
1.3.2.1. الهندسة الاجتماعية
2.3.2.1. الطرق الشائعة الاستخدام
3.1. تقنيات وأدوات الذكاء
1.3.1. استخبارات المصادر المفتوحة
2.3.1. ذكاء وسائل التواصل الاجتماعي
3.3.1. الاستخبارات البشرية
4.3.1. توزيعات وأدوات لينكس
5.3.1. منهجية تقييم الأمن اللاسلكي المفتوح
6.3.1. مشروع أمان تطبيق الويب المفتوح
7.3.1. معيار أداء اختبار الاختراق PTES
8.3.1. دليل منهجية اختبار الأمان مفتوح المصدر OSSTM
4.1. منهجيات التقييم
1.4.1. تحليل الذكاء
2.4.1. تقنيات تنظيم المعلومات المكتسبة
3.4.1. الموثوقية والمصداقية في مصادر المعلومات
4.4.1. منهجيات التحليل
5.4.1. عرض نتائج الذكاء

5.1. التدقيق والتوثيق
1.5.1. التدقيق فى أمن تكنولوجيا المعلومات
2.5.1. أذونات التوثيق والتدقيق
3.5.1. أنواع التدقيق
4.5.1. الإنجازات
1.4.5.1. تقرير تقني
2.4.5.1. البيان التنفيذي
6.1. عدم الكشف عن الهوية على الشبكة
1.6.1. استخدام عدم الكشف عن الهوية
2.6.1. تقنيات إخفاء الهوية (Proxy، VPN)، الشبكة الخصوصية الافتراضية)
3.6.1. شبكات TOR، مشروع الانترنت المخفية 2IP وFreenet
7.1. التهديدات وأنواع الأمن
1.7.1. أنواع التهديدات
2.7.1. الأمن المادي
3.7.1. الامن في الشبكات
4.7.1. الأمن المنطقي
5.7.1. الأمان في تطبيقات الويب
6.7.1. الأمن على الأجهزة المحمولة
8.1. اللوائح والامتثال compliance
1.8.1. النظام الأوروبي العام لحماية البيانات
2.8.1. المفهوم الإبداعي والاستراتيجية
3.8.1. مجموعة من المعايير الدولية لأمن المعلومات ISO 00072
4.8.1. إطار عمل الأمن الإلكترونى من المعهد الوطني للمعايير والتكنولوجيا
5.8.1. PIC
6.8.1. ISO 23072
7.8.1. لوائح *Cloud*
8.8.1. SOX
9.8.1. PCI
9.1. تحليل المخاطر والمعايير
1.9.1. مدى المخاطر
2.9.1. الأصول
3.9.1. التهديدات
4.9.1. نقاط الضعف
5.9.1. تقييم المخاطر
6.9.1. علاج المخاطر
10.1. منظمات مهمة في مجال الأمن السيبراني
1.10.1. إطار الأمن السيبرانيNIST
2.10.1. وكالة الاتحاد الأوروبي للأمن السيبراني
3.10.1. الإعلان والعواطف
4.10.1. .منظمة الدول الأمريكية
5.10.1. UNASUR - PROSUR.

الوحدة 2. أمان Host

1.2. نسخ احتياطية
1.1.2. استراتيجيات النسخ الاحتياطية
2.1.2. أدوات ويندوز
3.1.2. أدوات لنظام Linux
4.1.2. أدوات لنظام MacOS
2.2. برنامج مكافحة الفيروسات للمستخدم
1.2.2. أنواع مضادات الفيروسات
2.2.2. مضاد فيروسات Windows
3.2.2. مضاد فيروسات Linux
4.2.2. مضاد فيروسات لنظام MacOS
5.2.2. مضاد فيروسات للهواتف الذكية smartphones
3.2. أجهزة كشف التسلل - HIDS
1.3.2. طرق كشف التسلل
2.3.2. Sagan
3.3.2. Aide
4.3.2. Rkhunter

4.2. Firewall محلى

1.4.2. Firewalls لـ Windows

2.4.2. Firewalls لـ Linux

3.4.2. Firewalls لـ MacOS

5.2. مديرى كلمات المرور

1.5.2. Password

2.5.2. LastPass

3.5.2. KeePass

4.5.2. StickyPassword

5.5.2. RoboForm

6.2. أجهزة كشف التصيد phishing

1.6.2. الكشف اليدوي عن التصيد 1

2.6.2. أدوات antiphishing

7.2. برامج التجسس Spyware

1.7.2. آليات التجنب

2.7.2. أدوات مكافحة برامج التجسس antispyware

8.2. أجهزة التتبع

1.8.2. تدابير لحماية النظام

2.8.2. أدوات مكافحة التعقب

9.2. EDR End Point Detection and Response

1.9.2. سلوك نظام كشف نقطة النهاية والاستجابة لها

2.9.2. الاختلافات بين كشف نقطة النهاية والاستجابة لها ومكافحة الفيروسات

3.9.2. مستقبل أنظمة كشف نقطة النهاية والاستجابة لها

10.2. السيطرة على تثبيت البرنامج

1.10.2. المستودعات ومحلات البرمجيات

2.10.2. قوائم البرامج المسموح بها أو المحظورة

3.10.2. معايير التحديث

الوحدة 3. أمان الشبكة (المحيط)

1.3. أنظمة الكشف عن التهديدات والوقاية منها

1.1.3. الإطار العام للحوادث الأمنية

2.1.3. أنظمة الدفاع الحالية: Defense in Depth ومركز العمليات الأمنية

3.1.3. معماريات الشبكات الحالية

4.1.3. أنواع أدوات الكشف والوقاية من الحوادث

1.4.1.3. أنظمة قائمة على شبكات

2.4.1.3. أنظمة قائمة على المضيف

3.4.1.3. أنظمة مركزية

5.1.3. الاتصال واكتشاف الحالات/المضيفين والحاويات واللاسيرفرات،

2.3. Firewall

1.2.3. أنواع firewalls

2.2.3. الهجمات والتخفيف من آثارها

3.2.3. Firewalls الشائعة فى نواة (نظم تشغيل) kernel لينيكس

1.3.2.3. UFW

2.3.2.3. *Nftables* و *iptables*

3.3.2.3. Firewalld

4.2.3. أنظمة الكشف على أساس سجلات النظام

1.4.2.3. أغلفة بروتوكول التحكم بالنقل TCP Wrappers

2.4.2.3. BlockHosts وdenyHosts

3.4.2.3. ban2Fai

3.3. أنظمة كشف التسلل والوقاية منه

1.3.3. الهجمات على أنظمة كشف التسلل وأنظمة الوقاية منه

2.3.3. أنظمة كشف التسلل وأنظمة الوقاية منه

1.2.3.3. نظام كشف التسلل الأكثر شعبية

2.2.3.3. موتور كشف ومنع التسلل

الوحدة 4. أمن الهواتف الذكية smartphones

1.4. عالم الأجهزة النقالة
1.1.4. أنواع المنصات المحمولة
2.1.4. أجهزة Ios
3.1.4. أجهزة Android
2.4. إدارة أمن الأجهزة المحمولة
1.2.4. فتح مشروع أمان تطبيقات الويب على الأجهزة المحمولة
1.1.2.4. أهم 10 نقاط ضعف
2.2.4. الاتصالات والشبكات وأنماط الاتصال
3.4. الجهاز المحمول في بيئة الأعمال
1.3.4. المخاطر
2.3.4. مراقبة الاجهزة
3.3.4. إدارة البيانات الرئيسية (MDM)
4.4. خصوصية المستخدم وأمن البيانات
1.4.4. حالة المعلومات
2.4.4. حماية البيانات والسرية
1.2.4.4. الأذونات
2.2.4.4. التشفير
3.4.4. تخزين البيانات بشكل آمن
1.3.4.4. تخزين آمن في iOS
2.3.4.4. تخزين آمن في Android
4.4.4. الممارسات الجيدة في تطوير التطبيقات
5.4. نقاط الضعف ونواقل الهجوم
1.5.4. نقاط الضعف
2.5.4. نواقل الهجوم
1.2.5.4. البرمجيات الخبيثة
2.2.5.4. استخراج البيانات
3.2.5.4. التلاعب بالبيانات

4.3. Firewalls جدران الحماية من الجيل القادم
1.4.3. الاختلافات بين الجيل القادم من جدران الحماية وجدار الحماية التقليدي
2.4.3. القدرات الأساسية
3.4.3. حلول الأعمال
4.4.3. Firewalls للخدمات *Cloud*
1.4.4.3. Arquitectura Cloud سحابة أمازون الافتراضية الخاصة
2.4.4.3. سحابة قائمة نظام الدخول Cloud ACLs
3.4.4.3. Security Group
5.3. Proxy
1.5.3. أنواع proxy
2.5.3. استخدام proxy. المميزات والعيوب
6.3. محركات مكافحة الفيروسات
1.6.3. السياق العام للبرامج الضارة وبطاقات e
2.6.3. مشاكل محرك مكافحة الفيروسات
7.3. أنظمة حماية البريد
1.7.3. مكافحة البريد الغير مرغوب فيه Antispam
1.1.7.3. القوائم السوداء والبيضاء
2.1.7.3. مرشحات بايزي
2.7.3 . Mail Gateway (MGW)
8.3. المعلومات الأمنية وإدارة الأحداث
1.8.3. المكونات والعمارة
2.8.3. قواعد الارتباط وحالات الاستخدام
3.8.3. التحديات الحالية للمعلومات الأمنية وإدارة الأحداث
9.3. التنسيق الأمني والأتمتة والاستجابة
1.9.3. SOAR و SIEM: أعداء أو حلفاء
2.9.3. مستقبل أنظمة التنسيق الأمني والأتمتة والاستجابة
10.3. نظم أخرى قائمة في الشبكات
1.10.3. جدار الحماية لتطبيقات الويب
2.10.3. التحكم في الوصول إلى الشبكة
3.10.3. HoneyPots و HoneyNets
4.10.3. وسيط أمان الوصول إلى السحابة

6.4. التهديدات الرئيسية

1.6.4 . مستخدم غير مجبر

2.6.4 . البرمجيات الخبيثة

1.2.6.4. أنواع البرامج الضارة malware

3.6.4 . الهندسة الاجتماعية

4.6.4 . تسرب البيانات

5.6.4 . سرقة المعلومات

6.6.4 . شبكات لاسلكية wi-fi غير آمنة

7.6.4 . برامج غير محدثة

8.6.4 . تطبيقات خبيثة

9.6.4 . كلمات مرور ضعيفة

10.6.4. إعدادات أمان ضعيفة أو غير موجودة

11.6.4. الوصول المادي

12.6.4. فقدان أو سرقة الجهاز

13.6.4. سرقة الهوية (النزاهة)

14.6.4. تشفير ضعيف أو مكسور

15.6.4. رفض الخدمة (DoS)

7.4. الهجمات الرئيسية

1.7.4 . هجمات phishing

2.7.4 . الهجمات المتعلقة بأساليب الاتصال

3.7.4 . هجمات smishing

4.7.4 . هجمات من قبل criptojacking

5.7.4 . Man in The Middle

8.4. القرصنة Hacking

1.8.4. Rooting و jailbreaking

2.8.4. تشريح هجوم محمول

1.2.8.4. انتشار التهديد

2.2.8.4. تثبيت البرمجيات الخبيثة malware على الجهاز

3.2.8.4. المثابرة

4.2.8.4. تنفيذ payload واستخراج المعلومات

3.8.4. Hacking أجهزة iOS: الآليات والأدوات

4.8.4. Hacking أجهزة Android: الآليات والأدوات

9.4. اختبارات الاختراق

1.9.4. iOS PenTesting

2.9.4. Android pentesting

3.9.4. الأدوات

10.4. الحماية والأمن

1.10.4. اعدادات الامان

1.1.10.4. في أجهزة iOS

2.1.10.4. في أجهزة Android

2.10.4. إجراءات السلامة

3.10.4. أدوات الحماية

الوحدة 5. الأمن في إنترنت الأشياء IoT

1.5. الأجهزة

1.1.5. أنواع الأجهزة

2.1.5. هياكل قياسية

1.2.1.5. مشروع الشراكة العالمية

2.2.1.5. المنتدى العالمي لإنترنت الأشياء IoTWF

3.1.5. بروتوكولات التطبيق

4.1.5. تقنيات الاتصال

2.5. أجهزة إنترنت الأشياء. مجالات التطبيق

1.2.5. SmartHome

2.2.5. SmartCity

3.2.5. وسائل النقل

4.2.5 . الأجهزة القابلة للارتداء Wearables

5.2.5. قطاع الصحة

6.2.5. إنترنت الأشياء

3.5. بروتوكولات الاتصال

1.3.5. برتوكول MQTT

2.3.5. فتح بروتوكول تحالف المحمول

3.3.5. بروتوكول إدارة أجهزة تحالف الجوال المفتوح OMA-DM

4.3.5. التقرير الفني 960

الوحدة 6. Hacking أخلاقيات

1.6. بيئة العمل
1.1.6. توزيعات Linux
1.1.1.6. كالي لينكس - الأمن الهجومي
2.1.1.6. Parrot OS
3.1.1.6. نظام تشغيل متعدد الاستخدامات Ubuntu
2.1.6. أنظمة المحاكاة الافتراضية
3.1.6. صندوق الحماية
4.1.6. نشر المختبرات
2.6. المنهجيات
1.2.6. دليل منهجية اختبار الأمان مفتوح المصدر OSSTM
2.2.6. مشروع أمان تطبيقات الويب المفتوحة OWASP
3.2.6. إطار الأمن السيبراني NIST
4.2.6. معيار أداء اختبار الاختراق PTES
5.2.6. إطار عمل مفتوح المصدر للتحليل والاختبار الأمني ISSAF
3.6. بصمات الأقدام Footprinting
1.3.6. الاستخبارات مفتوحة المصدر (OSINT)
2.3.6. البحث عن الخروقات ونقاط الضعف في البيانات
3.3.6. استخدام الأدوات السلبية
4.6. مسح الشبكات
1.4.6. أدوات المسح
1.1.4.6. اختصار مخطط الشبكة
2.1.4.6. مولد حزم مفتوح المصدر
3.1.4.6. أدوات المسح الأخرى
2.4.6. تقنيات المسح
3.4.6. تقنيات النهرب من IDSg firewall
4.4.6. Banner grabbing
5.4.6. مخططات الشبكة

4.5. SmartHome
1.4.5. أتمتة المنزل
2.4.5. الشبكات
3.4.5. الأجهزة المنزلية
4.4.5. المراقبة والأمن
5.5. SmartCity
1.5.5. الإضاءة
2.5.5. علم الارصاد الجوية
3.5.5. الأمان
6.5. وسائل النقل
1.6.5. الموقع
2.6.5. سداد المدفوعات والحصول على الخدمات
3.6.5. الاتصال
7.5. الأجهزة القابلة للارتداء Wearables
1.7.5. ملابس ذكية
2.7.5. مجوهرات ذكية
3.7.5. الساعات الذكية
8.5. قطاع الصحة
1.8.5. مراقبة التمرين/معدل ضربات القلب
2.8.5. مراقبة المرضى وكبار السن
3.8.5. الغرسات
4.8.5. الروبوتات الجراحية
9.5. الاتصال
1.9.5. Wi-Fi/Gateway
2.9.5. بلوتوث
3.9.5. الاتصال المدمج
10.5. التأمين
1.10.5. الشبكات المعنية
2.10.5. مدير كلمات المرور
3.10.5. استخدام البروتوكولات المشفرة
4.10.5. نصائح الاستخدام

5.6. تعداد
1.5.6. تعداد SMTP
2.5.6. تعداد بروتوكول لنقل البريد البسيط DNS
3.5.6. تعداد بروتوكول إنترنت وسامبا (برنامج)
4.5.6. تعداد بروتوكول الوصول الى الدليل خفيف الوزن
5.5.6. تعداد بروتوكول إدارة الشبكات البسيطة
6.5.6. تقنيات التعداد الأخرى
6.6. فحص الثغرات الأمنية
1.6.6. حلول فحص الثغرات الأمنية
1.1.6.6. Qualys
2.1.6.6. نيساسNessus
3.1.6.6. إدارة التصحيح وفحص الثغرات الأمنية وتدقيق الشبكة
2.6.6. أنظمة تسجيل نقاط الضعف
1.2.6.6. نظام تسجيل نقاط الضعف المشتركة
2.2.6.6. نقاط الضعف والتعرضات الشائعة
3.2.6.6. قاعدة بيانات الضعف الوطنية
7.6. هجمات الشبكات اللاسلكية
1.7.6. منهجيات hacking فى الشبكات اللاسلكية
1.1.7.6. Wi-Fi Discovery
2.1.7.6. تحليل حركة المرور
3.1.7.6. هجمات aircrack
1.3.1.7.6. هجمات الشبكة العنكبوتية العالمية
2.3.1.7.6. هجمات وصول محمي للشبكات اللاسلكية / الوصول المحمي بتقنية Wi-Fi 2
4.1.7.6. هجمات Evil Twin
5.1.7.6. هجمات إعداد واي فاي المحمي
6.1.7.6. التشويش
2.7.6. أدوات الأمن اللاسلكية
8.6. القرصنة على خوادم الويب
1.8.6. Cross Site Scripting
2.8.6. تزوير الطلب عبر المواقع
3.8.6. Hijacking الجلسات
4.8.6. SQLinjection
9.6. استغلال نقاط الضعف
1.9.6. استخدام exploits المعروفة
2.9.6. استخدام metasploit
3.9.6. استخدامmalware
1.3.9.6. التعريف والنطاق
2.3.9.6. توليد malware
3.3.9.6. تجاوز حلول مكافحة الفيروسات
10.6. المثابرة
1.10.6. تركيب rootkits
2.10.6. استخدام ncat
3.10.6. استخدام المهام المجدولة backdoors
4.10.6. إنشاء المستخدم
5.10.6. .نظام كشف التسلل القائم على المضيف

الوحدة 7. الهندسة العكسية

1.7. المجمعين
1.1.7. أنواع الأكواد
2.1.7. مراحل مجمع البيانات
3.1.7. جدول الرموز
4.1.7. مدير الأخطاء
5.1.7. مجموعة مترجمات جنو
2.7. أنواع التحليل في المجمعين
1.2.7. تحليل معجمي
1.1.2.7. المصطلحات
2.1.2.7. المكونات المعجمية
3.1.2.7. محلل معجمي القانون الكنسي LEX
2.2.7. التحليل النحوي
1.2.2.7. قواعد نحوية خالية من السياق
2.2.2.7. أنواع التحليل النحوي
1.2.2.2.7. التحليل التنازلي
2.2.2.2.7. التحليل التصاعدي
3.2.2.7. أشجار النحو والاشتقاقات

4.2.2.7. أنواع المحللين النحويين

1.4.2.2.7. محللين مجزئ يسار يمين (Left To Right)

2.4.2.2.7. محلليين مجزئ يسار يمين

3.2.7. التحليل الدلالي

1.3.2.7. قواعد السمات

2.3.2.7. القواعد المنسوبة التي تحتوي على السمات المركبة S-atribuidas

3.3.2.7. القواعد المنسوبة التي تحتوي على السمات المركبة L-Atribuidas

3.7. هياكل بيانات المجمّع

1.3.7. المتغيرات

2.3.7. المصفوفات

3.3.7. المؤشرات

4.3.7. الهياكل

5.3.7. العناصر

4.7. هياكل الكود في المجمع

1.4.7. هياكل الاختيار

1.1.4.7. If، else if، Else

2.1.4.7. Switch

2.4.7. هياكل التكرار

1.2.4.7. For

2.2.4.7. While

3.2.4.7. استخدام break

3.4.7. المهام

5.7. بنية الأجهزة 68x

1.5.7. بنية المعالج 68x

2.5.7. بنية البيانات في 68x

3.5.7. بنية الكود فى 68x

6.7. بنية أجهزة معمارية ARM

1.6.7. بنية معالج معمارية ARM

2.6.7. بنية بيانات معمارية ARM

3.6.7. بنية الكود في معمارية ARM

7.7. تحليل الشفرة الثابتة

1.7.7. المفككات

2.7.7. المفكك التفاعلي IDA

3.7.7. معيدي بناء الكود

8.7. تحليل الشفرة الديناميكية

1.8.7. تحليل السلوك

1.1.8.7. الاتصالات

2.1.8.7. المراقبة

2.8.7. مصححات كود Linux

3.8.7. مصححات كود Windows

9.7. صندوق الحماية

1.9.7. هندسة معمارية sandbox

2.9.7. التهرب من sandbox

3.9.7. تقنيات الكشف

4.9.7. تقنيات التهرب

5.9.7. التدابير المضادة

6.9.7. Sandbox الحماية في Linux

7.9.7. صندوق الحماية في ويندوز

8.9.7. Sandbox فى MacOS

9.9.7. Sandbox في Android

10.7. تحليل البرامج الضارة

1.10.7. مناهج تحاليل *malware*

2.10.7. تقنيات تشويش البرمجيات الخبيثة *malware*

1.2.10.7. التعتيم على الملفات التنفيذية

2.2.10.7. تقييد بيئات التنفيذ

3.10.7. أدوات تحليل البرمجيات الخبيثة

الوحدة 8. التطوير الآمن

8.1. التطوير الآمن
1.1.8. الجودة والوظيفة والسلامة
2.1.8. السرية والنزاهة والتوافر
3.1.8. دورة حياة تطوير malware
2.8. مرحلة المتطلبات
1.2.8. التحكم في المصادقة
2.2.8. السيطرة على الأدوار والامتيازات
3.2.8. المتطلبات الموجهة للمخاطر
4.2.8. اعتماد الامتيازات
3.8. مرحلة التحليل والتصميم
1.3.8. الوصول إلى المكونات وإدارة النظام
2.3.8. مسارات التدقيق
3.3.8. إدارة الجلسات
4.3.8. بيانات تاريخية
5.3.8. التعامل السليم مع الأخطاء
6.3.8. الفصل بين الوظائف
4.8. مرحلة التنفيذ والتشفير
1.4.8. ضمان البيئة التطويرية
2.4.8. إعداد الوثائق الفنية
3.4.8. تشفير آمن
4.4.8. أمن الاتصالات
5.8. الممارسات الجيدة للتشفير الآمن
1.5.8. التحقق من صحة البيانات المدخلة
2.5.8. تشفير بيانات الإخراج
3.5.8. أسلوب البرمجة
4.5.8. إدارة سجل التغيير
5.5.8. ممارسات التشفير
6.5.8 . إدارة الأخطاء والسجلات
7.5.8. إدارة السجلات
8.5.8. إدارة الذاكرة
9.5.8. توحيد وإعادة استخدام وظائف الأمن
6.8. إعداد الخادم و hardening
1.6.8. إدارة المستخدمين والمجموعات والأدوار على الخادم
2.6.8. تثبيت البرامج
3.6.8. Hardening الخادم
4.6.8. اعداد قوي لبيئة التطبيق
7.8. إعداد قاعدة البيانات وتقويتها
1.7.8. تحسين محرك قاعدة البيانات
2.7.8. إنشاء مستخدم خاص للتطبيق
3.7.8. تعيين الامتيازات الدقيقة للمستخدم hardening من قواعد البيانات
8.8. مرحلة الإختبار
1.8.8. مراقبة الجودة في الضوابط الأمنية
2.8.8. فحص الرمز على مراحل
3.8.8. التحقق من إدارة التهيئة
4.8.8. اختبار الصندوق الأسود
9.8. تحضير خطوة الإنتاج
1.9.8. مراقبة التغيير
2.9.8. تنفيذ إجراء خطوة إلى الإنتاج
3.9.8. تنفيذ إجراء *rollback*
4.9.8. الاختبارات في مرحلة ما قبل الإنتاج
10.8. مرحلة الصيانة
1.10.8. التأمين على أساس المخاطر
2.10.8. اختبارات صيانة سلامة الصندوق الأبيض
3.10.8. اختبارات صيانة سلامة الصندوق الاسود

الوحدة 9. التحليل الجنائي

9.1. الحصول على البيانات ونسخها
9.1.1. الحصول على البيانات المتقلبة
9.1.1.1. معلومات النظام
9.1.1.2. معلومات الشبكة
9.1.1.3. ترتيب التقلب
9.2.1. الحصول على البيانات الثابتة
9.2.1.1. إنشاء صورة منسوخة
9.2.1.2. إعداد وثيقة لسلسلة الحيازة
9.3.1. طرق التحقق من صحة البيانات المكتسبة
9.3.1.1. منهجيات Linux
9.3.1.2. منهجيات Windows
9.2. تقييم وهزيمة تقنيات مكافحة الأدلة الجنائية
9.2.1. أهداف التقنيات امكافحة الأدلة الجنائية
9.2.2. مسح البيانات
9.2.2.1. حذف البيانات والملفات
9.2.2.2. استرجاع الملفات
9.2.2.3. استرجاع الأقسام المحذوفة
9.2.3. الحماية بكلمة مرور
9.2.4. إخفاء المعلومات
9.2.5. الحذف الآمن للأجهزة
9.2.6. التشفير
9.3. التحليل الجنائي لنظام التشغيل
9.3.1. التحليل الجنائي لنظام Windows
9.3.2. التحليل الجنائي لنظام Windows
9.3.3. التحليل الجنائي لنظام Mac
9.4. التحليل الجنائي للشبكة
9.4.1. تحليل السجلات
9.4.2. ترابط البيانات
9.4.3. بحث الشبكة
9.4.4. الخطوات الواجب اتباعها في التحليل الجنائي للشبكة
9.5. التحليل الجنائي للويب
9.5.1. التحقيق في هجمات الويب
9.5.2. كشف الهجمات
9.5.3. تعقب عناوين نظام منع الاختراق IPs
9.6. التحليل الجنائي لقواعد البيانات
9.6.1. التحليل الجنائي لبرنامج قواعد البيانات العلائقية MSSQL
9.6.2. التحليل الجنائي نظام إدارة قواعد البيانات MySQL
9.6.3. التحليل الجنائي في نظام إدارة قواعد البيانات PostgreSQL
9.6.4. التحليل الجنائي في نظام قاعدة بيانات مفتوحة المصدر MongoDB
9.7. التحليل الجنائي في Cloud
9.7.1. أنواع الجرائم فى Cloud
9.7.1.1. السحابة كمشتبه
9.7.1.2. السحابة كغرض
9.7.1.3. السحابة كأداة
9.7.2. تحديات التحليل الجنائى فى Cloud
9.7.3. البحث فى خدمات التخزين Cloud
9.7.4. أدوات الادلة الجنائية Cloud
9.8. التحقيق في جرائم البريد الإلكتروني
9.8.1. أنظمة البريد
9.8.1.1. عملاء البريد
9.8.1.2. خادم البريد
9.8.1.3. خادم البريد الصادر SMTP
9.8.1.4. خادم 3POP
9.8.1.5. خادم روتوكول الوصول إلى رسائل الإنترنت
9.8.2. جرائم البريد
9.8.3. رسالة بريدية
9.8.3.1. رؤوس قياسية
9.8.3.2. رؤوس ممتدة
9.8.4. خطوات التحقيق في هذه الجرائم
9.8.5. أدوات جنائية للبريد الإلكتروني

9.9. التحليل الجنائي للهواتف المحمولة
1.9.9. شبكات خلوية
1.1.9.9. أنواع الشبكات
2.1.9.9. محتويات إثبات الاستلام CDR
2.9.9. وحدة تعريف المشترك (SIM)
3.9.9. الاستحواذ المنطقي
4.9.9. الاستحواذ المادي
5.9.9. اكتساب نظام الملفات
10.9. صياغة تقارير التحليل الجنائي وتقديمها
1.10.9. الجوانب الهامة لتقرير التحليل الجنائي
2.10.9. تصنيف وأنواع التقارير
3.10.9. دليل لكتابة التقرير
4.10.9. عرض التقرير
1.4.10.9. التحضير المسبق للإدلاء بشهادة
2.4.10.9. الشهادة
3.4.10.9. التعامل مع الوسائط

الوحدة 10. التحديات الحالية والمستقبلية في أمن الحاسوب

1.10. تكنولوجيا بلوكشين blockchain
1.1.10. مجالات التطبيق
2.1.10. ضمان السرية
3.1.10. ضمان عدم التنصل
2.10. النقود الرقمية
1.2.10. عملات البيتكوين
2.2.10. العملات الرقمية
3.2.10. تعدين العملات المشفرة
4.2.10. عمليات احتيال الهرمي
5.2.10. الجرائم والمشاكل المحتملة الأخرى
3.10. Deepfake
1.3.10. تأثير الوسائط
2.3.10. مخاطر على المجتمع
3.3.10. آليات الكشف

4.10. مستقبل الذكاء الاصطناعي
1.4.10. الذكاء الاصطناعي والحوسبة المعرفية
2.4.10. استخدامات لتبسيط خدمة العملاء
5.10. الخصوصية الرقمية
1.5.10. قيمة البيانات على الشبكة
2.5.10. استخدام البيانات على الشبكة
3.5.10. إدارة الخصوصية والهوية الرقمية
6.10. النزاعات السيبرانية ومجرمين الإنترنت والهجمات الإلكترونية
1.6.10. تأثير الأمن السيبراني في النزاعات الدولية
2.6.10. عواقب الهجمات السيبراني على عموم السكان
3.6.10. أنواع مجرمي الإنترنت. إجراءات الحماية
7.10. العمل عن بعد
1.7.10. ثورة العمل عن بعد أثناء وبعد كوفيد-91
2.7.10. اختناقات الوصول
3.7.10. تباين سطح الهجوم
4.7.10. احتياجات العمال
8.10. التقنيات اللاسلكية الناشئة
1.8.10. الوصول إلى شبكة Wi-Fi المحمية 3
2.8.10. شبكة الجيل الخامس
3.8.10. موجات مليمترية
4.8.10. الاتجاه على Get Smart بدلاً من Get More
9.10. عنونة المستقبل في الشبكات
1.9.10. المشاكل الحالية مع عنونة نظام منع الاختراق
2.9.10. الإصدار السادس من بروتوكول الإنترنت
3.9.10. الإصدار الرابع من بروتوكول الإنترنت 4IPv+
4.9.10. مميزات الإصدار السادس من بروتوكول الإنترنت + الإصدار الرابع من بروتوكول الإنترنت
5.9.10. مميزات الإصدار السادس من بروتوكول الإنترنت 6IPv عن الإصدار الرابع من بروتوكول الإنترنت
10.10. التحدي المتمثل في زيادة الوعي بالتعليم المبكر والمستمر للسكان
1.10.10. الاستراتيجيات الحالية للحكومات
2.10.10. مقاومة السكان للتعلم
3.10.10. خطط التدريب التي يجب أن تتبناها الشركات

الوحدة 11. القيادة والأخلاق والمسؤولية الاجتماعية للشركة

1.11. العولمة والحكامة
1.1.11. الحكامة وادارة الشركات
2.1.11. أساسيات حوكمة الشركات في الشركات
3.1.11. دور مجلس الإدارة في إطار حوكمة الشركات
2.11. القيادة
1.2.11. القيادة. النهج المفاهيمي
2.2.11. القيادة في الشركات
3.2.11. أهمية القائد في إدارة الأعمال
3.11. Cross Cultural Management
1.3.11. مفهوم Cross Cultural Management
2.3.11. مساهمات في معرفة الثقافات الوطنية
3.3.11. إدارة التنوع
4.11. التنمية الإدارية والقيادة
1.4.11. مفهوم التنمية الإدارية
2.4.11. مفهوم القيادة
3.4.11. نظريات القيادة
4.4.11. أساليب القيادة
5.4.11. الذكاء في القيادة
6.4.11. .تحديات القائد اليوم
5.11. أخلاقيات العمل
1.5.11. الأخلاق والأخلاقيات
2.5.11. أخلاقيات الأعمال التجارية
3.5.11. القيادة والأخلاقيات في الشركة
6.11. الاستدامة
1.6.11. الاستدامة والتنمية المستدامة
2.6.11. أجندة 0302
3.6.11. الشركات المستدامة
7.11. المسؤولية الاجتماعية للشركة
1.7.11. البعد الدولي للمسؤولية الاجتماعية للشركات
2.7.11. زرع المسؤولية الاجتماعية للشركة
3.7.11. التأثير وقياس درجة المسؤولية الاجتماعية للشركات

8.11. أنظمة وأدوات الإدارة المسؤولة
1.8.11. المسؤولية الاجتماعية للشركات
2.8.11. القضايا الرئيسية في تنفيذ استراتيجية الإدارة المسؤولة
3.8.11. خطوات تطبيق نظام إدارة المسؤولية الاجتماعية للشركات
4.8.11. أدوات ومعايير المسؤولية الاجتماعية للشركات
9.11. الشركات متعددة الجنسيات وحقوق الإنسان
1.9.11. العولمة والشركات متعددة الجنسيات وحقوق الإنسان
2.9.11. الشركات متعددة الجنسيات مقابل القانون الدولي
3.9.11. الصكوك القانونية للشركات المتعددة الجنسيات فيما يتعلق بحقوق الإنسان
10.11. البيئة القانونية و Corporate Governance
1.10.11. لوائح الاستيراد والتصدير الدولية
2.10.11. الملكية الفكرية والصناعية
3.10.11. قانون العمل الدولي

الوحدة 12. قيادة الأفراد وإدارة المواهب

1.12. إدارة الأفراد الإستراتيجية
1.1.12. الإدارة الاستراتيجية للموارد البشرية
2.1.12. إدارة الأفراد الإستراتيجية
2.12. إدارة الموارد البشرية حسب الكفاءات
1.2.12. تحليل الكفائة
2.2.12. سياسة المكافآت
3.2.12. خطط التوظيف / التعاقب الوظيفي
3.12. تقييم الأداء وإدارة الأداء
1.3.12. ادارة الأداء
2.3.12. إدارة الأداء: الأهداف و العملية
4.12. الابتكار في إدارة المواهب والأفراد
1.4.12. نماذج إدارة المواهب الإستراتيجية
2.4.12. تحديد المواهب والتدريب والتطوير
3.4.12. الولاء والاحتفاظ
4.4.12. المبادرة والابتكار
5.12. تحفيز
1.5.12. طبيعة الدافع
2.5.12. نظرية التوقعات
3.5.12. نظريات الحاجيات
4.5.12. الدافع والتعويض المالي
6.12. تطوير فرق عالية الأداء
1.6.12. فرق عالية الأداء: فرق تدار ذاتيا
2.6.12. منهجيات إدارة الفريق ذاتية الإدارة عالي الأداء
7.12. إدارة التغيير
1.7.12. إدارة التغيير
2.7.12. أنواع عملية إدارة التغيير
3.7.12. فترات أو مراحل في إدارة التغيير
8.12. التفاوض وإدارة النزاعات
1.8.12. التفاوض
2.8.12. إدارة النزاعات
3.8.12. إدارة الأزمات
9.12. التواصل الإداري
1.9.12. التواصل الداخلي والخارجي في الأعمال التجارية
2.9.12. أقسام التواصل
3.9.12. مدير الإعلامات في الشركة ملف تعريف مدير التواصل في الشركة
10.12. إنتاجية المواهب وجذبها والاحتفاظ بها وتفعيلها
1.10.12. الإنتاجية
2.10.12. عوامل جذب المواهب والاحتفاظ بها

الوحدة 13. الإدارة الاقتصادية والمالية

13.1. البيئة الاقتصادية
1.1.13. بيئة الاقتصاد الكلي والنظام المالي الوطني
2.1.13. المؤسسات المالية
3.1.13. الأسواق المالية
4.1.13. الأصول المالية
5.1.13. الجهات الأخرى في القطاع المالي

2.13. المحاسبة الإدارية
1.2.13. مفاهيم أساسية
2.2.13. أصول الشركة
3.2.13. التزامات الشركة
4.2.13. الميزانية الرئيسية للشركة
5.2.13. كشف الدخل
3.13. أنظمة المعلومات Business Intelligence (ذكاء الأعمال)
1.3.13. الأساسيات والتصنيف
2.3.13. مراحل وطرق تقاسم التكلفة
3.3.13. اختيار مركز التكلفة والتأثير
4.13. مراقبة الميزانية والإدارة
1.4.13. نموذج الميزانية
2.4.13. الميزانية الرأسمالية
3.4.13. الميزانية التشغيلية
5.4.13. ميزانية الخزينة
6.4.13. تتبع الميزانية
5.13. الإدارة المالية
1.5.13. القرارات المالية للشركة
2.5.13. قسم المالية
3.5.13. الفوائض النقدية
4.5.13. المخاطر المرتبطة بالإدارة المالية
5.5.13. إدارة مخاطر الإدارة المالية
6.13. التخطيط المالي
1.6.13. تعريف التخطيط المالي
2.6.13. الإجراءات الواجب اتخاذها في التخطيط المالي
3.6.13. إنشاء استراتيجية العمل ووضعها
4.6.13. جدول التدفق النقدى Cash Flow
5.6.13. الجدول الحالي
7.13. الاستراتيجية المالية للشركة
1.7.13. الاستراتيجية المؤسسية ومصادر التمويل
2.7.13. المنتجات المالية لتمويل الأعمال
8.13. التمويل الاستراتيجي
1.8.13. التمويل الذاتي
2.8.13. زيادة الأموال الخاصة
3.8.13. الموارد الهجينة
4.8.13. التمويل عن طريق الوسطاء
9.13. التحليل المالي والتخطيط
1.9.13. تحليل الميزانية العمومية
2.9.13. تحليل قائمة الدخل
3.9.13. تحليل الربحية
10.13. تحليل وحل الحالات/ المشاكل
1.10.13. المعلومات المالية لشركة التصميم وصناعة النسيج S.A. (INDITEX)

الوحدة 14. الإدارة التجارية والتسويق الاستراتيجي

14.1. الإدارة التجارية
1.1.14. الإطار المفاهيمي للإدارة التجارية
2.1.14. استراتيجية الأعمال والتخطيط
3.1.14. دور المديرين التجاريين
2.14. Marketing
1.2.14. مفهوم التسويق
2.2.14. عناصر التسويق الأساسية
3.2.14. الأنشطة التسويقية للشركة
3.14. إدارة التسويق الاستراتيجي
1.3.14. مفهوم التسويق الاستراتيجي
2.3.14. مفهوم التخطيط الاستراتيجي للتسويق
3.3.14. مراحل عملية التخطيط التسويقي الاستراتيجي
4.14. التسويق الرقمي والتجارة الإلكترونية
1.4.14. أهداف التسويق الرقمي والتجارة الإلكترونية
2.4.14. التسويق الرقمي والوسائط المستخدمة
3.4.14. التجارة الإلكترونية. السياق العام
4.4.14. فئات التجارة الإلكترونية
5.4.14. مزايا وعيوب التجارة الإلكترونيةEcommerce مقابل التجارة التقليدية

5.14. التسويق الرقمي لتقوية العلامة التجارية
1.5.14. استراتيجيات عبر الإنترنت لتحسين سمعة علامتك التجارية
2.5.14. Branded Content & Storytelling
6.14. التسويق الرقمي لجذب العملاء والاحتفاظ بهم
1.6.14. استراتيجيات الولاء والمشاركة عبر الإنترنت
2.6.14. إدارة علاقات الزوار
3.6.14. التجزئة المفرطة
7.14. ادارة الحملات الرقمية
1.7.14. ما هي الحملة الإعلانية الرقمية؟
2.7.14. خطوات إطلاق حملة تسويق عبر الإنترنت
3.7.14. أخطاء في الحملات الإعلانية الرقمية
8.14. استراتيجية المبيعات
1.8.14. استراتيجية المبيعات
2.8.14. طرق البيع
9.14. التواصل المؤسساتي
1.9.14. المفهوم
2.9.14. أهمية الإعلام في المؤسسة
3.9.14. نوع الإعلام في المنظمة
4.9.14. وظائف الإعلام في المؤسسة
5.9.14. عناصر الإعلام
6.9.14. مشاكل الإعلام
7.9.14. سيناريوهات الإعلام
10.14. التواصل والسمعة الرقمية
1.10.14. السمعة عبر الانترنت
2.10.14. كيفية قياس السمعة الرقمية؟
3.10.14. أدوات السمعة عبر الإنترنت
4.10.14. تقرير السمعة عبر الإنترنت
5.10.14. Branding عبر الإنترنت

الوحدة 15. Management الاداري

15.1. General Management
1.1.15. مفهوم General Management
2.1.15. عمل Manager General
3.1.15. المدير العام ومهامه
4.1.15. تحويل عمل الإدارة
2.15. المدير ووظائفه. الثقافة التنظيمية ومقارباتها
1.2.15. المدير ووظائفه. الثقافة التنظيمية ومقارباتها
3.15. إدارة العمليات
1.3.15. أهمية الإدارة
2.3.15. سلسلة القيم
3.3.15. إدارة الجودة
4.15. الخطابة وتشكيل متحدثين رسميين
1.4.15. التواصل بين الأشخاص
2.4.15. مهارات التواصل والتأثير
3.4.15. حواجز التواصل
5.15. أدوات التواصل الشخصية والمؤسساتية
1.5.15. التواصل بين الأشخاص
2.5.15. أدوات التواصل بين الأشخاص
3.5.15. التواصل في المنظمات
4.5.15. الأدوات في المنظمة
6.15. التواصل في حالات الأزمات
1.6.15. الأزمات
2.6.15. مراحل الأزمات
3.6.15. الرسائل: المحتويات واللحظات
7.15. إعداد خطة للأزمات
1.7.15. تحليل المشاكل المحتملة
2.7.15. التخطيط
3.7.15. تكيف الموظفين

8.15. الذكاء العاطفي
1.8.15. الذكاء العاطفي والتواصل
2.8.15. الحزم والتعاطف والاستماع الفعال
3.8.15. الثقة بالنفس والإعلام العاطفي
9.15. Branding الشخصى
1.9.15. استراتيجيات لتطوير علامتك التجارية الشخصية
2.9.15. قوانين العلامات التجارية الشخصية
3.9.15. أدوات بناء العلامة التجارية الشخصية
10.15. القيادة وإدارة الفرق
1.10.15. القيادة وأساليب القيادة
2.10.15. قدرات القائد والتحديات
3.10.15. إدارة عملية التغيير
4.10.15. إدارة فرق متعددة الثقافات

مستقبلك يبدأ من هنا. سجّل اليوم لتصبح مدير أمن المعلومات في الشركات الكبرى"

06
المنهجية

يقدم هذا البرنامج التدريبي طريقة مختلفة للتعلم. فقد تم تطوير منهجيتنا من خلال أسلوب التعليم المرتكز على التكرار: ***Relearning*** أو ما يعرف بمنهجية إعادة التعلم.

يتم استخدام نظام التدريس هذا، على سبيل المثال، في أكثر كليات الطب شهرة في العالم، وقد تم اعتباره أحد أكثر المناهج فعالية في المنشورات ذات الصلة مثل مجلة نيو إنجلند الطبية ***(New England Journal of Medicine)***.

اكتشف منهجية *Relearning* (منهجية إعادة التعلم)، وهي نظام يتخلى عن التعلم الخطي التقليدي ليأخذك عبر أنظمة التدريس التعليم المرتكزة على التكرار: إنها طريقة تعلم أثبتت فعاليتها بشكل كبير، لا سيما في المواد الدراسية التي تتطلب الحفظ"

منهج دراسة الحالة لوضع جميع محتويات المنهج في سياقها المناسب

يقدم برنامجنا منهج ثوري لتطوير المهارات والمعرفة. هدفنا هو تعزيز المهارات في سياق متغير وتنافسي ومتطلب للغاية.

> مع جامعة TECH يمكنك تجربة طريقة تعلم تهز أسس الجامعات التقليدية في جميع أنحاء العالم"

سيتم توجيهك من خلال نظام التعلم القائم على إعادة التأكيد على ما تم تعلمه، مع منهج تدريس طبيعي وتقدمي على طول المنهج الدراسي بأكمله.

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

منهج تعلم مبتكرة ومختلفة

إن هذا البرنامج المُقدم من خلال TECH هو برنامج تدريس مكثف، تم خلقه من الصفر، والذي يقدم التحديات والقرارات الأكثر تطلبًا في هذا المجال، سواء على المستوى المحلي أو الدولي. تعزز هذه المنهجية النمو الشخصي والمهني، متخذة بذلك خطوة حاسمة نحو تحقيق النجاح. ومنهج دراسة الحالة، وهو أسلوب يرسي الأسس لهذا المحتوى، يكفل اتباع أحدث الحقائق الاقتصادية والاجتماعية والمهنية.

> يعدك برنامجنا هذا لمواجهة تحديات جديدة في بيئات غير مستقرة ولتحقيق النجاح في حياتك المهنية"

كان منهج دراسة الحالة هو نظام التعلم الأكثر استخدامًا من قبل أفضل كليات الحاسبات في العالم منذ نشأتها. تم تطويره في عام 1912 بحيث لا يتعلم طلاب القانون القوانين بناءً على المحتويات النظرية فحسب، بل اعتمد منهج دراسة الحالة على تقديم مواقف معقدة حقيقية لهم لاتخاذ قرارات مستنيرة وتقدير الأحكام حول كيفية حلها. في عام 1924 تم تحديد هذه المنهجية كمنهج قياسي للتدريس في جامعة هارفارد.

أمام حالة معينة، ما الذي يجب أن يفعله المهني؟ هذا هو السؤال الذي سنواجهك بها في منهج دراسة الحالة، وهو منهج تعلم موجه نحو الإجراءات المتخذة لحل الحالات. طوال المحاضرة الجامعية، سيواجه الطلاب عدة حالات حقيقية. يجب عليهم دمج كل معارفهم والتحقيق والجدال والدفاع عن أفكارهم وقراراتهم.

منهجية إعادة التعلم *(Relearning)*

تجمع جامعة TECH بين منهج دراسة الحالة ونظام التعلم عن بعد، 100٪ عبر الانترنت والقائم على التكرار، حيث تجمع بين عناصر مختلفة في كل درس.

نحن نعزز منهج دراسة الحالة بأفضل منهجية تدريس 100٪ عبر الانترنت في الوقت الحالي وهي: منهجية إعادة التعلم والمعروفة بـ *Relearning*.

في عام 2019، حصلنا على أفضل نتائج تعليمية متفوقين بذلك على جميع الجامعات الافتراضية الناطقة باللغة الإسبانية في العالم.

في TECH ستتعلم بمنهجية رائدة مصممة لتدريب مدراء المستقبل. وهذا المنهج، في طليعة التعليم العالمي، يسمى *Relearning* أو إعادة التعلم.

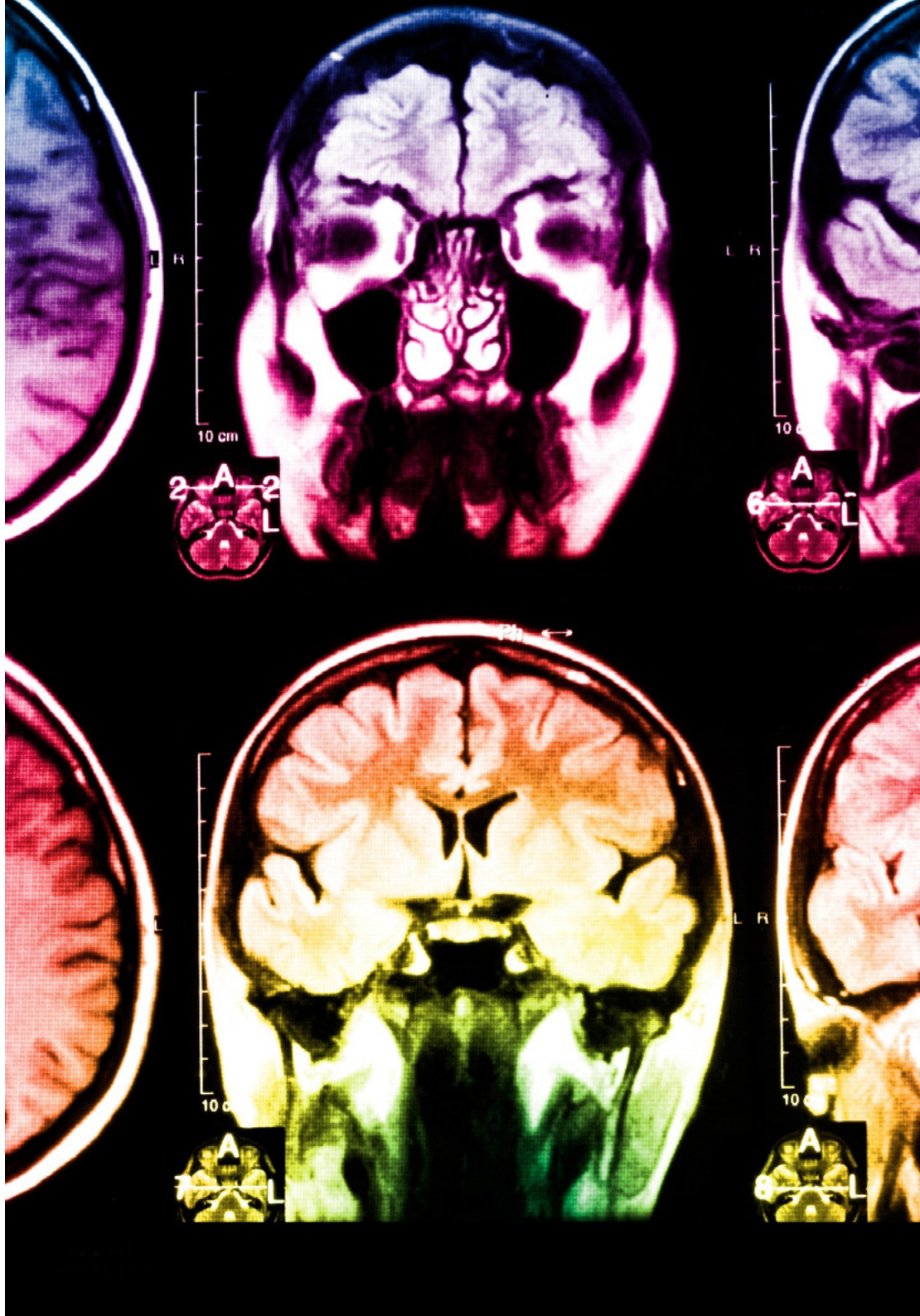
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلّم ثم نطرح ماتعلمناه جانبًا فننساه ثم نعيد تعلمه). لذلك، نقوم بدمج كل عنصر من هذه العناصر بشكل مركزي. باستخدام هذه المنهجية، تم تدريب أكثر من 650000 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 ذلك في بيئة شديدة المتطلبات، مع طلاب جامعيين يتمتعون بمظهر اجتماعي واقتصادي مرتفع ومتوسط عمر يبلغ 43.5 عاماً.

ستتيح لك منهجية إعادة التعلم والمعروفة بـ *Relearning*، التعلم بجهد أقل ومزيد من الأداء، وإشراكك بشكل أكبر في تدريبك، وتنمية الروح النقدية لديك، وكذلك قدرتك على الدفاع عن الحجج والآراء المتباينة: إنها معادلة واضحة 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 هو ضروريًا لكي نكون قادرين على تذكرها وتخزينها في الحُصين بالمخ، لكي نحتفظ 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 المُعَدَّة بعناية للمهنيين:

المواد الدراسية

يتم إنشاء جميع محتويات التدريس من قبل المتخصصين الذين سيقومون بتدريس البرنامج الجامعي، وتحديداً من أجله، بحيث يكون التطوير التعليمي محددًا وملموسًا حقًا.

ثم يتم تطبيق هذه المحتويات على التنسيق السمعي البصري الذي سيخلق منهج جامعة TECH في العمل عبر الإنترنت. كل هذا بأحدث التقنيات التي تقدم أجزاء عالية الجودة في كل مادة من المواد التي يتم توفيرها للطالب.

المحاضرات الرئيسية

هناك أدلة علمية على فائدة المراقبة بواسطة الخبراء كطرف ثالث في عملية التعلم.

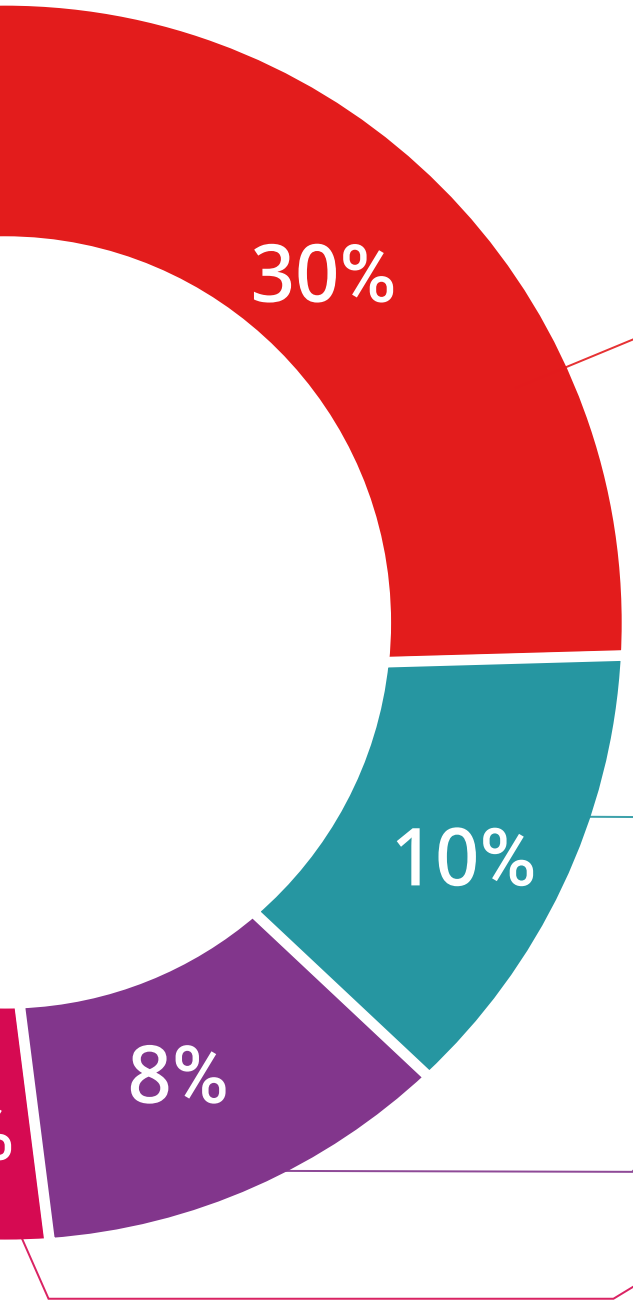
إن مفهوم ما يسمى *Learning from an Expert* أو التعلم من خبير يقوي المعرفة والذاكرة، ويولد الثقة في القرارات الصعبة في المستقبل.

التدريب العملي على المهارات والكفاءات

سيقومون بتنفيذ أنشطة لتطوير مهارات وقدرات محددة في كل مجال مواضيعي. التدريب العملي والديناميكيات لاكتساب وتطوير المهارات والقدرات التي يحتاجها المتخصص لنموه في إطار العولمة التي نعيشها.

قراءات تكميلية

المقالات الحديثة، ووثائق اعتمدت بتوافق الآراء، والأدلة الدولية. من بين آخرين. في مكتبة جامعة TECH الافتراضية، سيتمكن الطالب من الوصول إلى كل ما يحتاجه لإكمال تدريبه.



دراسات الحالة (Case studies)

سيقومون بإكمال مجموعة مختارة من أفضل دراسات الحالة المختارة خصيصًا لهذا المؤهل. حالات معروضة ومحللة ومدروسة من قبل أفضل المتخصصين على الساحة الدولية.

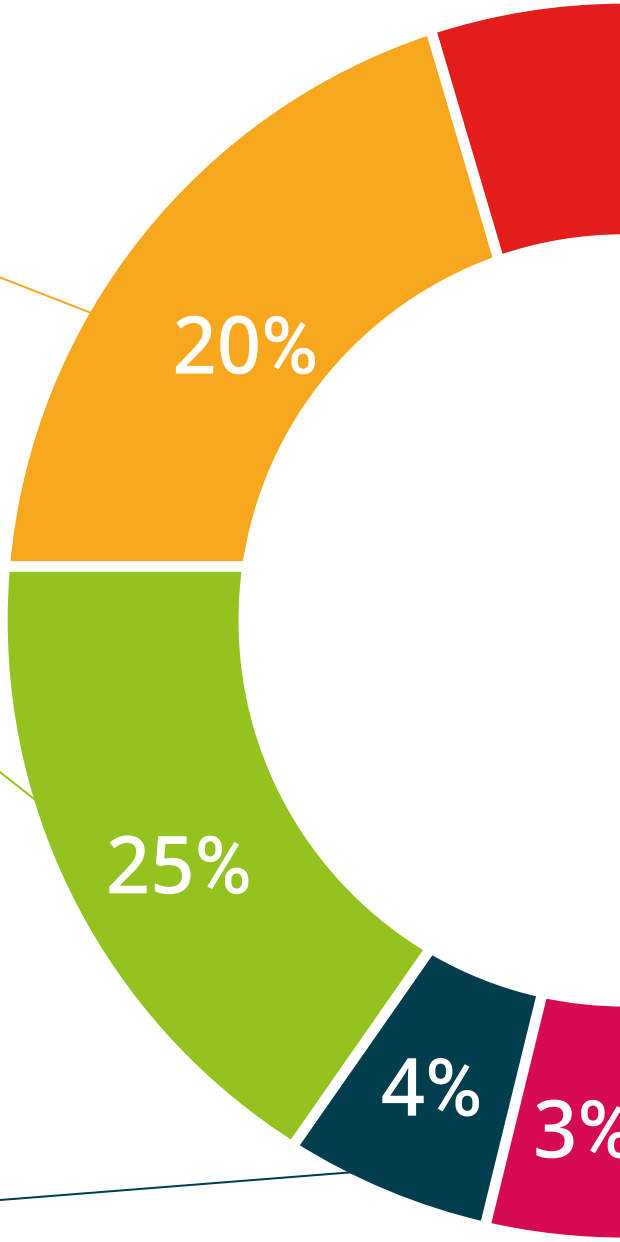
ملخصات تفاعلية

يقدم فريق جامعة TECH المحتويات بطريقة جذابة وديناميكية في أقراص الوسائط المتعددة التي تشمل الملفات الصوتية والفيديوهات والصور والرسوم البيانية والخرائط المفاهيمية من أجل تعزيز المعرفة.

اعترفت شركة مايكروسوف بهذا النظام التعليمي الفريد لتقديم محتوى الوسائط المتعددة على أنه "قصة نجاح أوروبية"

الاختبار وإعادة الاختبار

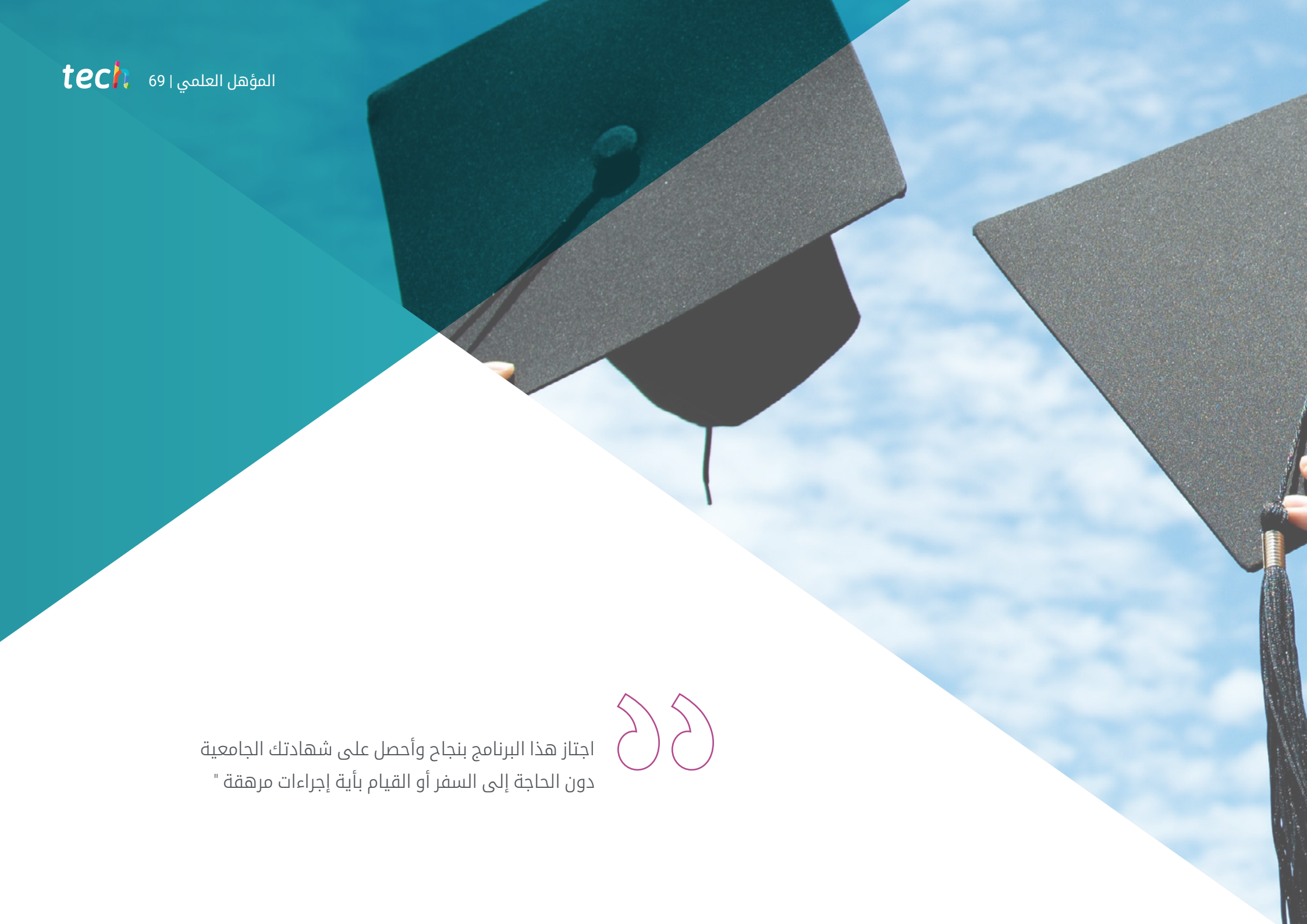
يتم بشكل دوري تقييم وإعادة تقييم معرفة الطالب في جميع مراحل البرنامج، من خلال الأنشطة والتدريبات التقييمية وذاتية التقييم: حتى يتمكن من التحقق من كيفية تحقيق أهدافه.



07

المؤهل العلمي

يضمن ماجستير خاص في MBA إدارة الأمن السيبراني (CISO، مدير أمن المعلومات)، بالإضافة إلى التدريب الأكثر دقة وحداثة، الحصول على درجة الماجستير الخاص الصادرة TECH الجامعة التكنولوجية.



اجتاز هذا البرنامج بنجاح وأحصل على شهادتك الجامعية
دون الحاجة إلى السفر أو القيام بأية إجراءات مرهقة "

هذه **ماجستير خاص في MBA إدارة الأمن السيبراني (CISO، مدير أمن المعلومات)** على البرنامج العلمي الأكثر اكتمالا وحداثة في السوق.

بعد اجتياز التقييم، سيحصل الطالب عن طريق البريد العادي* مصحوب بعلم وصول مؤهل **ماجستير خاص** الصادرعن **TECH الجامعة التكنولوجية**

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

المؤهل العلمي: **ماجستير خاص في MBA إدارة الأمن السيبراني (CISO، مدير أمن المعلومات)**

اطريقة: **عبر الإنترنت**

مدة: **12 شهر**


tech الجامعة التكنولوجية

شهادة تخرج

هذه الشهادة ممنوحة إلى

لـ

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

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

ماجستير خاص

في

MBA إدارة الأمن السيبراني
(CISO، مدير أمن المعلومات)

وهي شهادة خاصة من هذه الجامعة موافقة لـ 1500
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 خاص في MBA إدارة الأمن السيبراني (CISO، مدير أمن المعلومات)

التوزيع العام للخطة الدراسية

نوع المادة	عدد الساعات
(OB) إجباري	1500
(OP) إختياري	0
(PR) الممارسات الخارجية	0
(TFM) مشروع تخرج الماجيستير	0
الإجمالي	1500

التوزيع العام للخطة الدراسية

الدورة	المادة	الطريقة	عدد الساعات
1°	الذكاء والأمن السيبراني	إجباري	100
1°	أمان Host	إجباري	100
1°	أمان الشبكة (المحيط)	إجباري	100
1°	أمن الهواتف الذكية smartphones	إجباري	100
1°	الأمن فى إنترنت الأشياء IoT	إجباري	100
1°	Hacking لخلاقيات	إجباري	100
1°	الهندسة العكسية	إجباري	100
1°	التطوير الأمن	إجباري	100
1°	التحليل الجنائي	إجباري	100
1°	التحديات الحالية والمستقبلية فى أمن الحاسوب	إجباري	100
1°	القيادة والأخلاق والمسؤولية الاجتماعية للشركة	إجباري	100
1°	قيادة الأفراد وإدارة المواهب	إجباري	100
1°	الإدارة الاقتصادية والمالية	إجباري	100
1°	الإدارة التجارية والتسويق الاستراتيجي	إجباري	100
1°	Management الادارى	إجباري	100

tech الجامعة التكنولوجية

أ. د./ Tere Guevara Navarro
رئيس الجامعة

*تصديق الهاية ابوستيل. في حالة قيام الطالب بالتقدم للحصول على درجته العلمية الورقية وبتصديق لاهاي أبوستيل، ستتخذ مؤسسة TECH EDUCATION الإجراءات المناسبة لكي يحصل عليها وذلك بتكلفة إضافية.

الجامعة التيكنولوجية

ماجستير خاص
MBA إدارة الأمن السيبراني (CISO، مدير أمن المعلومات)

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **12 شهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

ماجستير خاص
MBA إدارة الأمن السيبراني
(CISO، مدير أمن المعلومات)

tech الجامعة التيكنولوجية