# محاضرة جامعية

# الأمن السيبراني في الهواتف الذكية

الجامعة التيكنولوجية

الجامعة التيكنولوجية

## محاضرة جامعية

# الأمن السيبراني في الهواتف الذكية

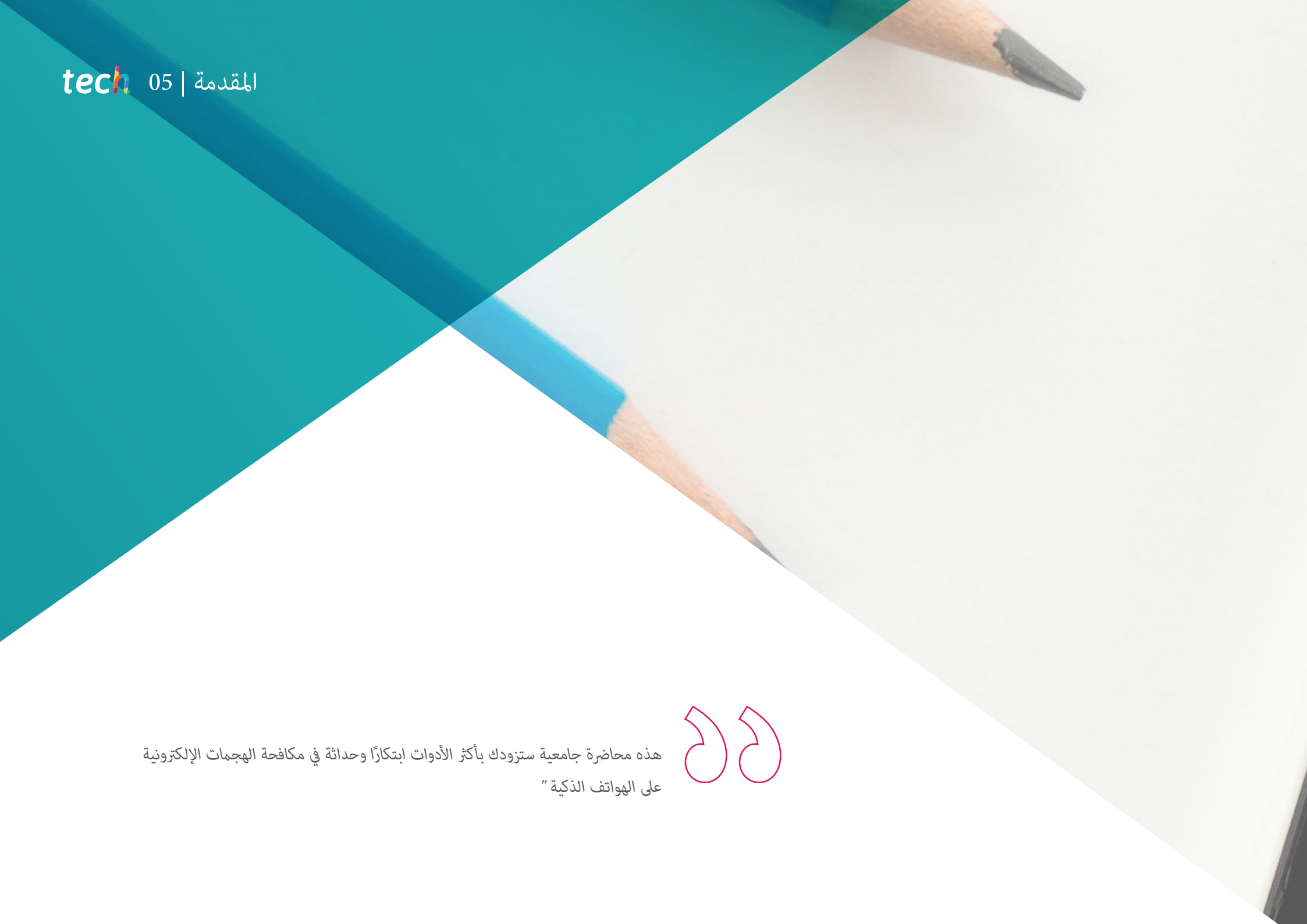
- طريقة التدريس: **أونلاين**
- مدة الدراسة: **6 أسابيع**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- عدد الساعات المخصصة للدراسة: **16 ساعات أسبوعيًا**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

رابط الدخول إلى الموقع الإلكتروني: **www.techtitute.com/ae/information-technology/postgraduate-certificate/smartphone-cybersecurity**

# الفهرس

# 01
# المقدمة

يجبر استخدام الأجهزة المحمولة المستخدمين على تحمل مستوى من المخاطر فيما يتعلق بحماية بياناتهم الشخصية والتي قد تكون عالية جدًا في بعض الحالات. يزيد الذكاء المتزايد لهذه الأجهزة أو الهواتف أو الأجهزة اللوحية أيضًا من سطح الهجوم المرتبط بها مما يفتح نقاط ضعف جديدة يمكن أن تصبح جرائم تصل حتى إلى سرقة الهوية أو السرقة أو الاحتيال. لمكافحتها يضطر متخصص الأمن السيبراني إلى العمل بالتوازي مع ظهور المخاطر وتطوير استجابات الحماية باستمرار. هذا البرنامج هو أداة تضع أحدث ما في هذا المجال في أيدي المتخصصين من أجل تمكينهم من تقديم حلول فعالة ومبتكرة.



هذه محاضرة جامعية ستزودك بأكثر الأدوات ابتكارًا وحداثة في مكافحة الهجمات الإلكترونية على الهواتف الذكية"

نحن نعيش في وقت يتزايد فيه انتشار استخدام الأجهزة المحمولة. منذ زمن بعيد توقف الهاتف عن كونه مجرد هاتف ليصبح حاسوبًا صغيرًا قادرًا على تصفح الإنترنت في أي وقت وتشغيل التطبيقات من جميع الأنواع وتحديد موقعنا على الخريطة والتخطيط للطرق وتخزين البيانات داخليًا وخارجيًا وأكثر بكثير من ذلك. عندما نتحدث عن هذه الأجهزة فإننا لا نشير فقط إلى الهواتف المحمولة بل نقوم بتضمين الأجهزة اللوحية. كل من الجهاز والآخر عبارة عن أجهزة مصممة ومجهزة لجعل حياتنا أسهل. بفضلهم يمكننا التحرك بسهولة والوصول إلى الشبكة في جميع الأوقات بالإضافة إلى الخدمات السحابية التي يزداد الطلب عليها.

يجب ألا ننسى أنه بفضل كل هذا"الذكاء" ازداد سطح الهجوم على هذه الأجهزة بشكل كبير من 0 إلى 100 وأن استخدامها المكثف جعلها هدفًا سهلاً. أصبحت الأجهزة المحمولة الآن الهدف الأساسي للمهاجمين الذين يسعون لانتهاك الخصوصية وسرقة الهوية وسرقة البيانات والوصول دون موافقة المستخدم واستخدام مالكي هذه الأجهزة لأغراض إجرامية.

لذلك من الأساسي والضروري تمامًا أن نضع جميع التدابير تحت تصرفنا لحماية خصوصيتنا. الأمن بنسبة 100٪ غير موجود ولكن إذا عرفنا أنواع الهجمات التي نواجهها والمخاطر التي نتعرض لها ولدينا المعلومات اللازمة للتعامل معها فسنكون قد اتخذنا خطوة مهمة وأضفنا طبقة أخرى من الأمان لمعلوماتنا.

تحتوي **محاضرة جامعية في الأمن السيبراني في الهواتف الذكية** على البرنامج العلمي الأكثر اكتمالاً وحداثةً في السوق. ومن أبرز الميزات:

- تطوير الحالات العملية التي يقدمها الخبراء في الأمن السيبراني
- 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
- 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

> اكتسب المعرفة اللازمة لتطوير نظام فعال لحماية الطبقة في غضون أسابيع قليلة من العمل"

المعلومات التي يحتاجها المحترف لإنشاء أنظمة حماية تضمن السلامة في استخدام الهاتف الذكي في برنامج تدريبي عالي"

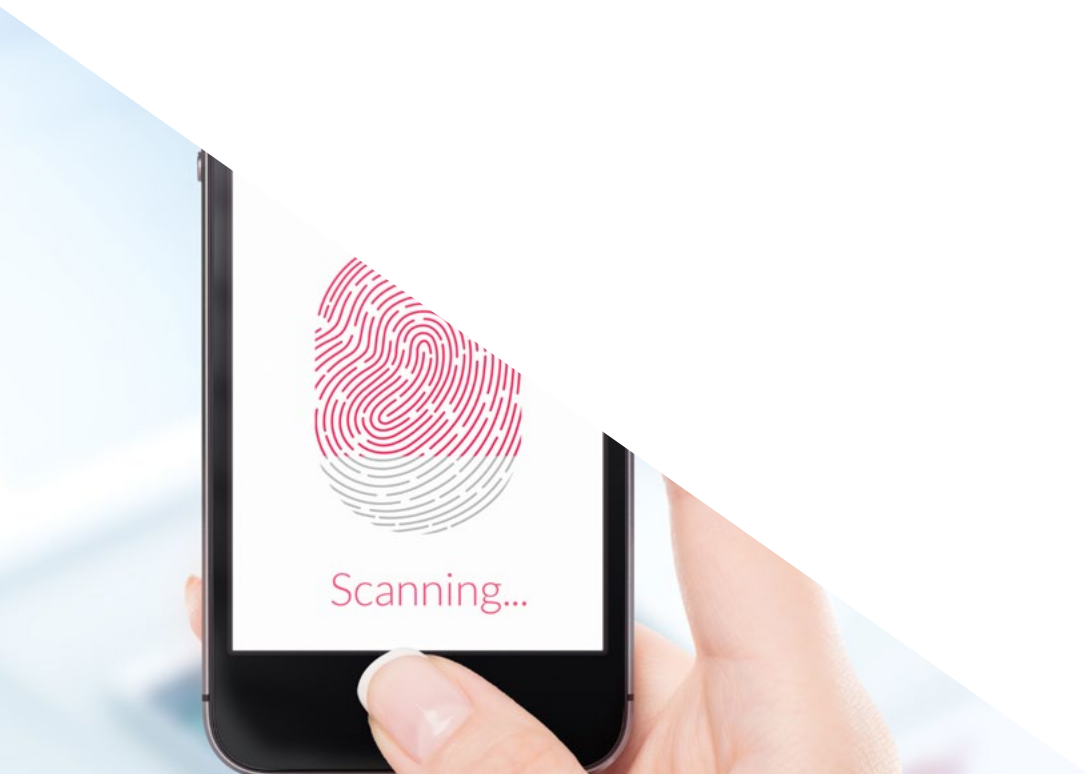
ادرس من خلال هذه محاضرة جامعية التركيز على الممارسة مما سيعزز قدرتك على المستوى التخصصي.

عملية مدربة تدريباً عالياً تم إنشاؤها لتكون سهلة الإدارة ومرنة مع منهجية التدريس عبر الإنترنت الأكثر إثارة للاهتمام

البرنامج يضم في هيئة التدريس متخصصين في المجال والذين يصبون خبراتهم العملية في هذا التدريب بالإضافة إلى متخصصين معترف بهم من مجتمعات رائدة وجامعات مرموقة.

سيسمح 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 المهني من خلاله محاولة حل الحالات المختلفة للممارسة المهنية التي تُطرَح على مدار هذا البرنامج. للقيام بذلك سيحصل على مساعدة من نظام جديد من مقاطع الفيديو التفاعلية التي أعدها خبراء معترف بهم.



02

# الأهداف

توفر هذه محاضرة جامعية في الأمن السيبراني في الهواتف الذكية للطلاب القدرة على العمل في هذا المجال بسرعة وسهولة. مع الغايات واقعية ومثيرة للاهتمام تم تكوين عملية الدراسة هذه طريقة لجلب الطلاب بشكل تدريجي لاكتساب المعرفة النظرية والعملية اللازمة للتدخل بالجودة، والتطوير، بالإضافة إلى الكفاءات المستعرضة التي تسمح التعامل مع المواقف المعقدة من خلال وضع استجابات معدلة ودقيقة.

ضع قدراتك موضع التنفيذ في مجال عمل مليء بإمكانيات التوظيف من خلال عملية تدريس ذات جودة استثنائية"

## الأهداف العامة

- تحليل منصات المحمول الرئيسية الحالية وخصائصها واستخداماتها
- فحص نقاط الضعف والتهديدات الموجودة بالإضافة إلى نواقل الهجوم الرئيسية
- تقييم المخاطر المرتبطة بنقاط الضعف خارج الشركة وداخلها
- تحديد الأدوات وأدلة الممارسات الجيدة لتحقيق حماية الأجهزة المحمولة

بالتفكير في الطالب تطبق هذه محاضرة جامعية أنظمة دعم
الدراسة الأكثر إثارة للاهتمام في الوقت الحالي"

## الأهداف المحددة

- 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

03

# هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

تم اختيار المعلمين الذين يقومون بتدريس هذا البرنامج لكفاءتهم الاستثنائية في هذا المجال. إنهم يجمعون بين الخبرة الفنية والعملية مع التدريس ويقدمون للطلاب دعمًا من الدرجة الأولى في تحقيق أهدافهم. من خلالهم يقدم البرنامج الرؤية الأكثر مباشرة وفورية للخصائص الحقيقية للتدخل في هذا المجال وتحقيق رؤية سياقية ذات أهمية قصوى.

سيرافقك مدرسون خبراء في الأمن السيبراني في كل مرحلة من مراحل الدراسة وسيمنحونك الرؤية الأكثر واقعية لهذا العمل"

## 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

### أ. Fernández Sapena, Sonia

- مدربة أمن الكمبيوتر و القرصنة الأخلاقية. مركز خيتافي المرجعي الوطني في الحوسبة والاتصالات. مدريد
- مدربة معتمدة من المجلس الإلكتروني. مدريد
- مدرب في الشهادات التالية: EXIN Ethical Hacking Foundation والمؤسسة الأمنية EXIN Cyber & IT. مدريد
- مدربة خبيرة معتمدة 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)، مشغلة شبكات الصوت والبيانات (IFCM0110)، وإدارة خدمات الإنترنت ( IFCT0509)
- متعاونة خارجية CSO/SSA (كبيرة مسؤولي الأمن / مهندسة أمنية أولى). جامعة Islas Baleares
- مهندسة كمبيوتر. جامعة Alcalá de Henares. مدريد
- ماجستير في DevOps: Docker and Kubernetes. Cas-Training. مدريد
- تقنيات أمان Microsoft Azure. E-Council. مدريد

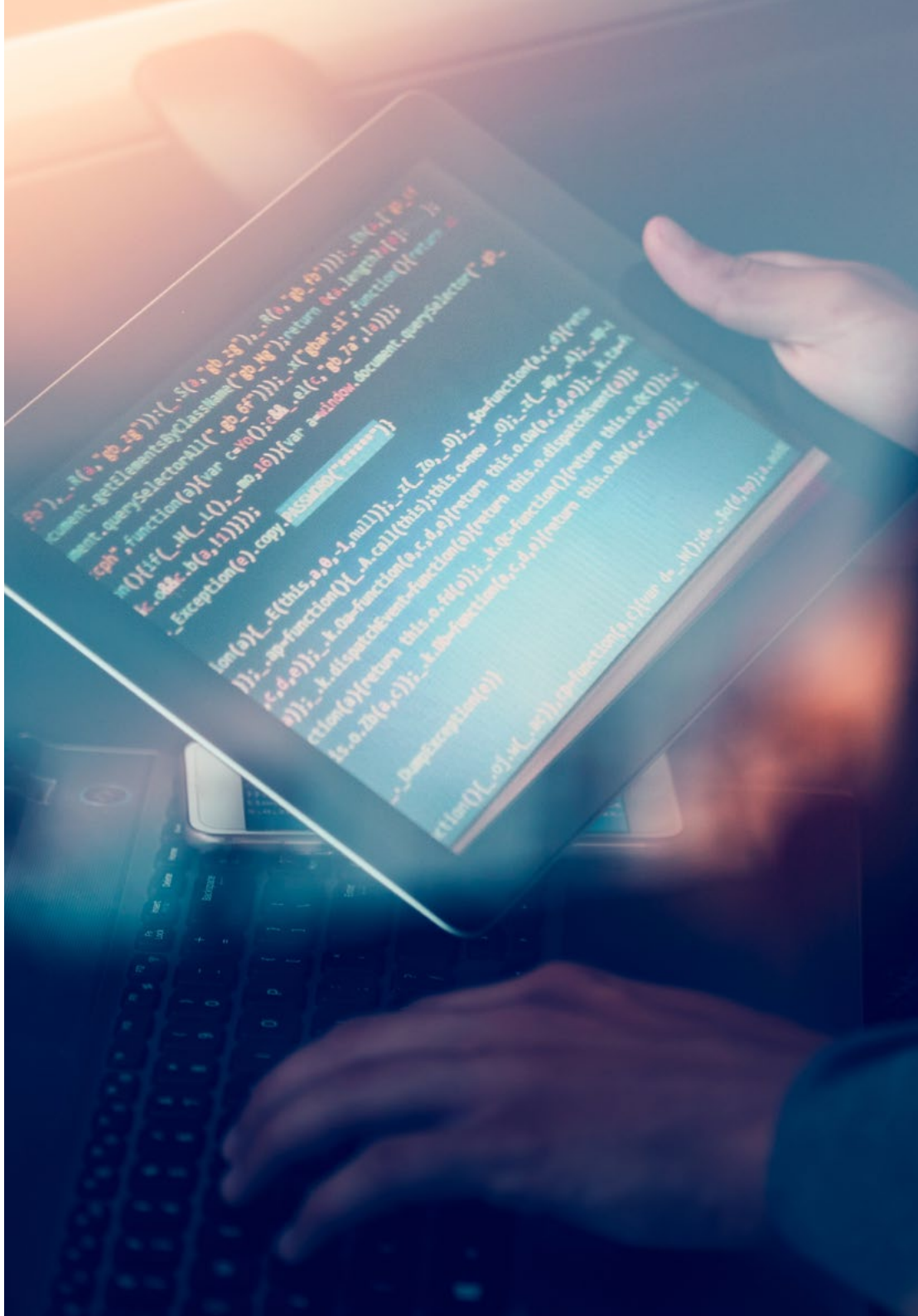
## الأساتذة

### أ. Marcos Sbarbaro, Victoria Alicia

- مطورة تطبيقات Android Mobile الأصلي في B60. المملكة المتحدة
- محللة ومبرمجة لإدارة وتنسيق وتوثيق البيئة الافتراضية لإنذارات أمان العميل
- محللة ومبرمجة لتطبيقات Java لأجهزة الصراف الآلي للعملاء
- محترفة تطوير البرمجيات لتطبيق التحقق من صحة التوقيع وإدارة الوثائق للعميل
- فنية أنظمة لترحيل المعدات وللإدارة والصيانة وتدريب الأجهزة المساعدة الرقمية الشخصية المحمولة للعميل
- الهندسة الفنية لأنظمة الكمبيوتر. جامعة Oberta كاتالونيا
- درجة ماجستير في أمن الكمبيوتر والقرصنة الأخلاقية الرسمية EC-Council و CompTIA من المدرسة المهنية للتكنولوجيات الجديدة CICE

### أ. Catalá Barba, José Francisco

- قيادي وسيط في MINIDEF. المهام والمسؤوليات المختلفة داخل GOE III مثل الإدارة وإدارة الحوادث للشبكة الداخلية وتنفيذ برامج مخصصة لمناطق مختلفة ودورات تدريبية لمستخدمي الشبكة وموظفي المجموعة بشكل عام
- فني الكتروني في مصنع Ford الموجود في Almusafes في فالنسيا وبرمجة الروبوت PLC بالإضافة إلى الاصلاح والصيانة
- فني الكتروني
- مطور لتطبيقات الجوال



04

# الهيكل والمحتوى

خلال التقدم في الموضوعات المختلفة لهذا المقرر سيكون الطالب قادرًا على اكتساب كل المعرفة التي يتطلبها تطوير أنظمة الأمان في الهواتف الذكية. لهذا فقد تم تنظيمه بهدف اكتساب التعلم التكميلي بكفاءة مما يعزز اختراق التعلم ويعزز ما تم دراسته مما يمنح الطلاب القدرة على التدخل في أسرع وقت ممكن. دورة مكثفة وجودة عالية تم إنشاؤها لتدريب أفضل في هذا القطاع.


تم تطوير جميع جوانب التدخل في الأمن السيبراني في الهواتف الذكية بطريقة منظمة في نهج دراسة يركز على الكفاءة"

## الوحدة 1. أمان الهاتف الذكي

1.1. عالم الهواتف المحمولة
1.1.1. أنواع المنصات المتنقلة
2.1.1. أجهزة iOS
3.1.1. أجهزة Android
2.1. إدارة أمن الأجهزة المحمولة
1.2.1. مشروع OWASP للأمان على الأجهزة المحمولة
1.1.2.1. أهم 10 نقاط ضعف
2.2.1. الاتصالات والشبكات وأنماط الاتصال
3.1. الجهاز المحمول في بيئة الأعمال
1.3.1. المخاطر
2.3.1. السياسة الأمنية
3.3.1. مراقبة الجهاز
4.3.1. إدارة الأجهزة المحمولة (MDM)
4.1. خصوصية المستخدم وأمن البيانات
1.4.1. حالة المعلومات
2.4.1. حماية البيانات والسرية
1.2.4.1. أذونات
2.2.4.1. التشفير
3.4.1. تخزين آمن للبيانات
1.3.4.1. تخزين آمن في iOS
2.3.4.1. تخزين آمن في Android
4.4.1. الممارسات الجيدة في تطوير التطبيقات
5.1. نقاط الضعف ونواقل الهجوم
1.5.1. نقاط الضعف
2.5.1. نواقل الهجوم
1.2.5.1. البرمجيات الضارة
2.2.5.1. استخراج البيانات
3.2.5.1. التلاعب بالبيانات
6.1. التهديدات الرئيسية
1.6.1. مستخدم غير مقيد
2.6.1. البرمجيات الضارة
1.2.6.1. أنواع البرمجيات الضارة
3.6.1. الهندسة الاجتماعية
4.6.1. تسرب البيانات
5.6.1. سرقة المعلومات
6.6.1. شبكات Wi-Fi غير آمنة
7.6.1. البرمجيات الغير مُحَدَثة
8.6.1. التطبيقات الضارة
9.6.1. كلمات السر الضعيفة
10.6.1. إعدادات الأمان ضعيفة أو غير موجودة
11.6.1. الوصول المادي
12.6.1. جهاز مفقود أو مسروق
31.6.1. انتحال الهوية (النزاهة)
41.6.1. تشفير ضعيف أو معطل
51.6.1. رفض الخدمة (DoS)
7.1. الهجمات الرئيسية
1.7.1. هجمات التصيد الاحتيالي
2.7.1. الهجمات المتعلقة بأساليب الاتصال
3.7.1. هجمات الرسائل القصيرة الاحتيالية
4.7.1. هجمات التعدين السري
5.7.1. الرجل في الوسط *Man in The Middle*
8.1. القرصنة
1.8.1. التجذير و كسر الحماية
2.8.1. تشريح الهجوم المحمول
1.2.8.1. انتشار التهديد
2.2.8.1. تثبيت البرمجيات الضارة على الجهاز
3.2.8.1. المثابرة
4.2.8.1. تنفيذ الحمولة واستخراج المعلومات
3.8.1. القرصنة على أجهزة iOS: الآليات والأدوات
4.8.1. القرصنة على أجهزة Android: الآليات والأدوات

9.1. اختبارات الاختراق

1.9.1. اختبار المكافحة على iOS

2.9.1. اختبار المكافحة على Android

3.9.1. أدوات

10.1. الحماية والأمن

1.10.1. اعدادات الامان

1.1.10.1. على أجهزة iOS

2.1.10.1. على أجهزة Android

2.10.1. تدابير أمنية

3.10.1. أدوات الحماية

"جميع أدوات التحليل والتطورات والحماية للهواتف الذكية من خلال موضوع يحظى باهتمام كبير وموضوعي تمامًا"

05

# 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.

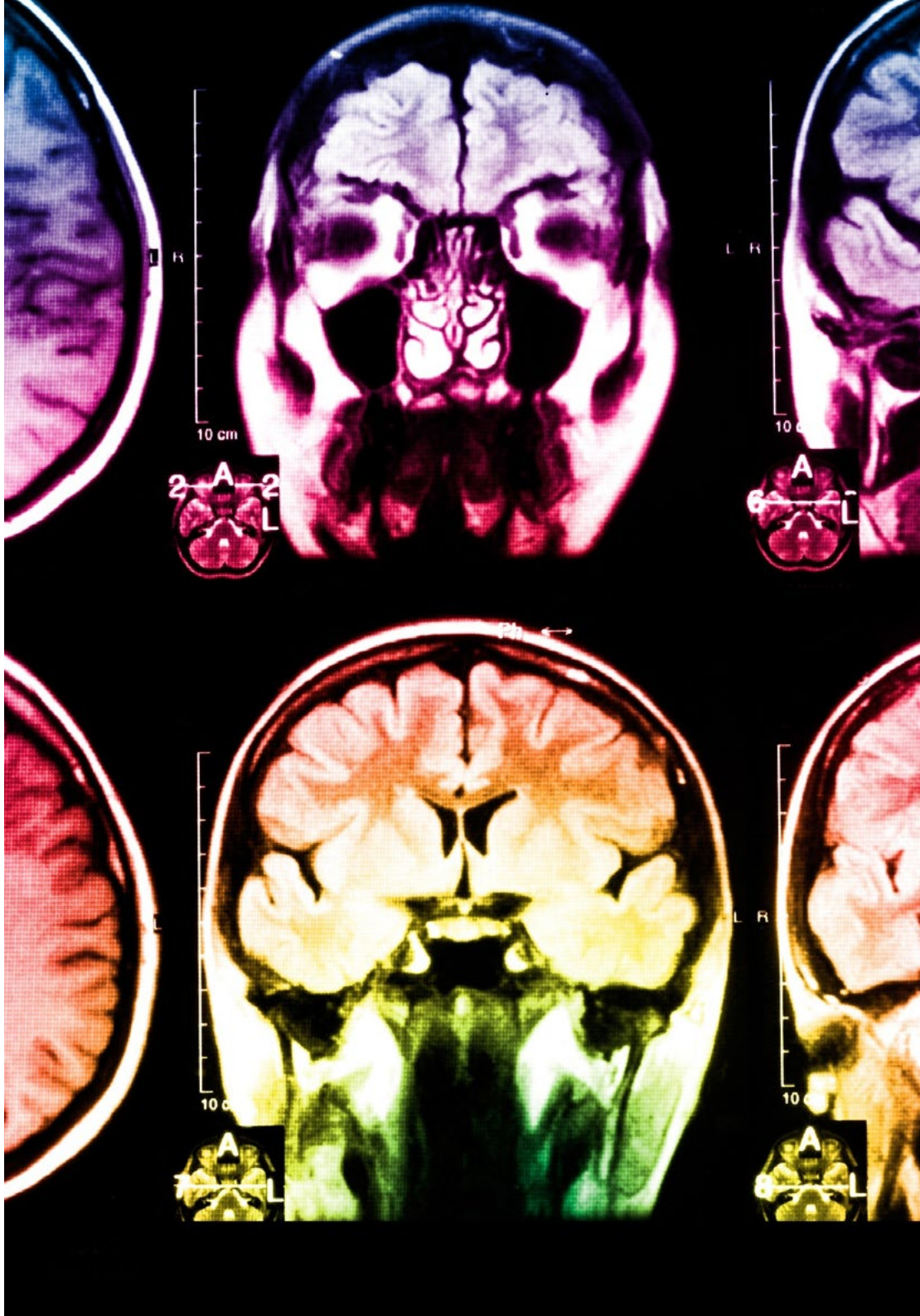
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

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.

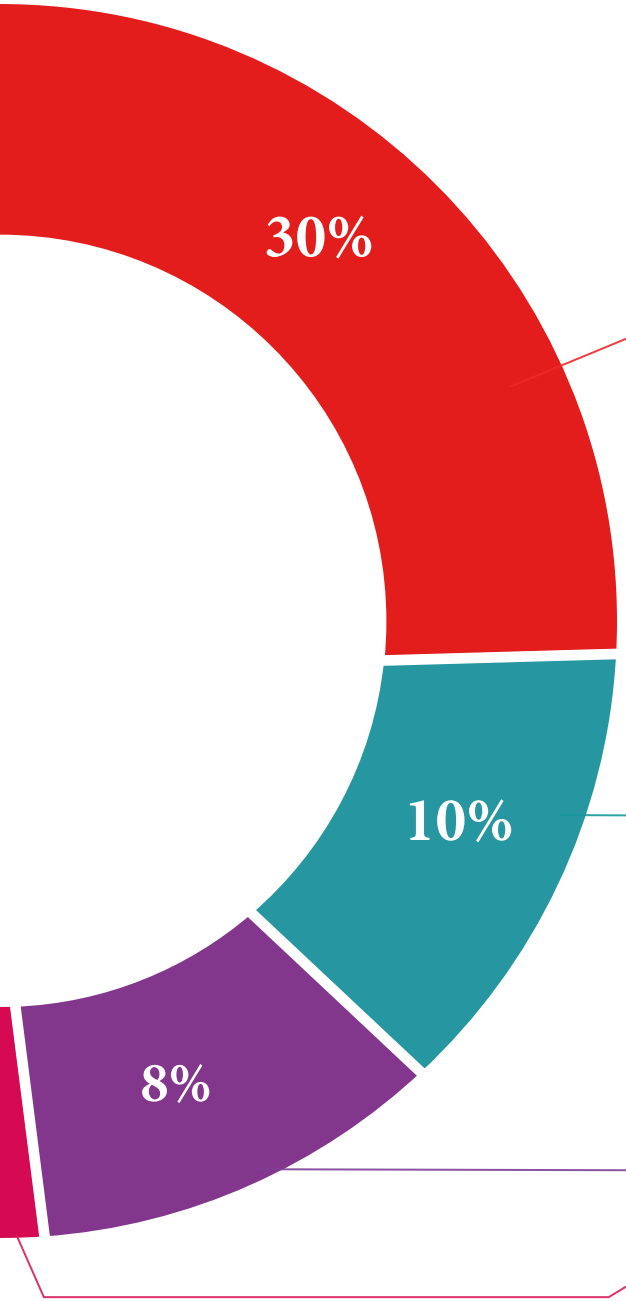
ستتيح لك منهجية إعادة التعلم والمعروفة بـ *Relearning*، التعلم بجهد أقل ومزيد من الأداء، وإشراكك بشكل أكبر في تدريبك، وتنمية الروح النقدية لديك، وكذلك قدرتك على الدفاع عن الحجج والآراء المتباينة: إنها معادلة واضحة للنجاح.

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

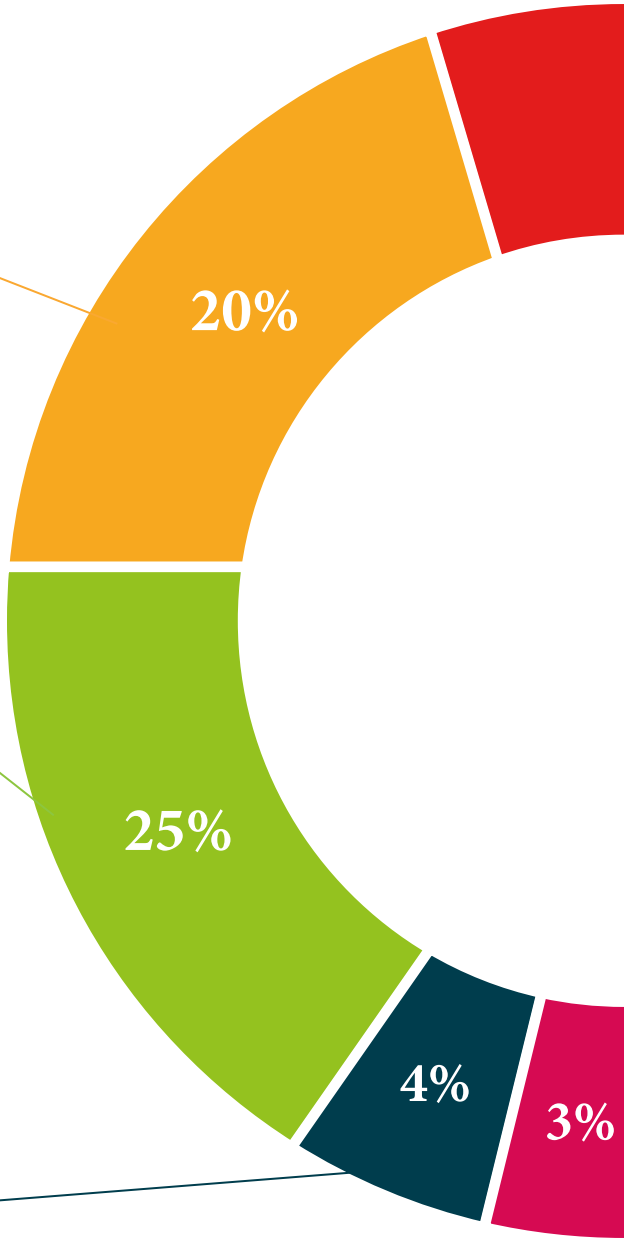
### ملخصات تفاعلية

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



06

# المؤهل العلمي

تضمن محاضرة جامعية في الأمن السيبراني في الهواتف الذكية، بالإضافة إلى التدريب الأكثر دقة وحداثة، الحصول على شهادة اجتياز محاضرة جامعية الصادرة عن TECH الجامعة التكنولوجية.

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

تحتوي **محاضرة جامعية في الأمن السيبراني في الهواتف الذكية** على البرنامج العلمي الأكثر اكتمالاً وحداثةً في السوق.

بعد اجتياز الطالب للتقييمات، سوف يتلقى عن طريق البريد العادي* مصحوب بعلم وصول مؤهل **محاضرة جامعية** ذا الصلة الصادر عن **TECH الجامعة التكنولوجية.**

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

المؤهل العلمي: **محاضرة جامعية في الأمن السيبراني في الهواتف الذكية**

عدد الساعات الدراسية المعتمدة: **150 ساعة**


tech الجامعة التكنولوجية

يمنح هذا

الدبلوم

لـ

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

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

محاضرة جامعية

في

الأمن السيبراني في الهواتف الذكية

وهي شهادة خاصة من هذه الجامعة موافقة لـ 150 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

*تصديق لاهاي أبوستيل. 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

## محاضرة جامعية

# الأمن السيبراني في الهواتف الذكية

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **6 أسابيع**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- عدد الساعات المخصصة للدراسة: **16 ساعات أسبوعيًا**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

# محاضرة جامعية

# الأمن السيبراني في الهواتف الذكية

tech الجامعة التيكنولوجية