شهادة الخبرة الجامعية
أمن الحاسوب للاتصالات

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

شهادة الخبرة الجامعية
أمن الحاسوب للاتصالات

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **6 اشهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

رابط الدخول إلى الموقع الإلكتروني: www.techtitute.com/ae/information-technology/postgraduate-diploma/postgraduate-diploma-computer-security-communications

الفهرس

01

المقدمة

يعد الاستخدام غير المصرح به وغير السليم للشبكات إحدى المشاكل الرئيسية التي قد يواجهها المستخدمون. من الضروري تنفيذ الإجراءات الأمنية للكمبيوتر، حيث تنتقل كمية كبيرة من المعلومات الخاصة والسرية عبر الإنترنت. تقرب شهادة الخبرة الجامعية الطلاب من مجال أمن الحاسوب للاتصالات من خلال برنامج حديث وعالي الجودة. إنه إعداد كامل يسعى إلى تدريب الطلاب على النجاح في مهنتهم.

إذا كنت تبحث عن برنامج التدريب عالي الجودة يساعدك على التخصص في أحد المجالات ذات الفرص الأكثر احترافًا، فهذا هو أفضل خيار لك"

تشهد التطورات في مجال الاتصالات تطوراً مستمراً، حيث يعد هذا المجال من أسرع المجالات تطوراً، لذلك من الضروري وجود خبراء في تكنولوجيا المعلومات قادرين على التكيف مع هذه التغييرات ولديهم معرفة مباشرة بالأدوات والتقنيات الجديدة التي تظهر في هذا المجال.

ضمن هذا المجال، يجب أن يكون أمن الحاسوب أحد الجوانب التي يجب على الشركات أن توليها أكبر قدر من الاهتمام، حيث أن جميع معلوماتها موجودة على الشبكة، ويمكن أن يشكل وصول المستخدم غير المنضبط لتنفيذ مهام غير مشروعة مشكلة خطيرة للمؤسسة، سواء من الناحية المالية أو من حيث السمعة.

تتناول شهادة الخبرة الجامعية في أمن الحاسوب للاتصالات مجموعة كاملة من القضايا التي ينطوي عليها هذا المجال. تقدم دراستها ميزة واضحة على الدورات التدريبية الأخرى التي تركز على كتل محددة، مما يمنع الطالب من معرفة العلاقات المتبادلة مع المجالات الأخرى المدرجة في مجال الاتصالات متعدد التخصصات. علاوة على ذلك، قام فريق التدريس في هذا البرنامج التعليمي باختيار دقيق لكل موضوع من موضوعات هذا التدريب لمنح الطالب فرصة دراسية كاملة قدر الإمكان ومرتبطة دائمًا بالأحداث الجارية.

يستهدف هذا البرنامج المهتمين بتحقيق مستوى أعلى من المعرفة في أمن الكمبيوتر للاتصالات. الهدف الرئيسي هو تدريب الطالب لتطبيق المعرفة المكتسبة في شهادة الخبرة الجامعية في العالم الحقيقي، في بيئة عمل تعيد إنتاج الظروف التي يمكن العثور عليها في المستقبل، بصرامة وواقعية.

تجدر الإشارة إلى أنه نظرًا لكونها شهادة الخبرة الجامعية 100% عبر الإنترنت، فإن الطالب غير مشروط بجداول زمنية ثابتة أو يحتاج إلى الانتقال إلى مكان مادي آخر، ولكن يمكنه الوصول إلى المحتويات في أي وقت من اليوم، وموازنة عملك أو حياتك الشخصية مع الحياة الأكاديمية.

تحتوي **شهادة الخبرة الجامعية في أمن الحاسوب للاتصالات** على البرنامج الأكثر اكتمالاً وحداثة في السوق أبرز خصائصها هي:

- تطوير الحالات العملية التي يقدمها خبراء في الأمان المعلوماتية
- المحتويات الرسومية والتخطيطية والعملية البارزة التي يتم تصورها بها، تجمع المعلومات العلمية والعملية حول تلك التخصصات الأساسية للممارسة المهنية
- التمارين العملية حيث يمكن إجراء عملية التقييم الذاتي لتحسين التعلم
- تركيزها بشكل خاص على المنهجيات المبتكرة في تدريس أمن الحاسوب للاتصالات
- 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

> لا تفوت فرصة تنفيذ شهادة الخبرة الجامعية في أمن الحاسوب للاتصالات معنا. إنها فرصة مثالية للتقدم في حياتك المهنية"

تعد شهادة الخبرة الجامعية هذه أفضل استثمار يمكنك القيام به في اختيار برنامج تحديث لتحديث معرفتك في أمن الحاسوب للاتصالات"

يضم في هيئة التدريس متخصصين ينتمون إلى مجال الحوسبة الاتصالات، والذين يجلبون خبراتهم العملية إلى هذا التدريب، 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 المحترف على مساعدة من نظام فيديو تفاعلي جديد تم تصميمه بواسطة خبراء معترف بهم في أمن الحاسوب للاتصالات ويتمتعون بخبرة واسعة.

يحتوي هذا التدريب على أفضل المواد التعليمية، والتي ستسمح لك بدراسة سياقية من شأنها تسهيل التعلم.

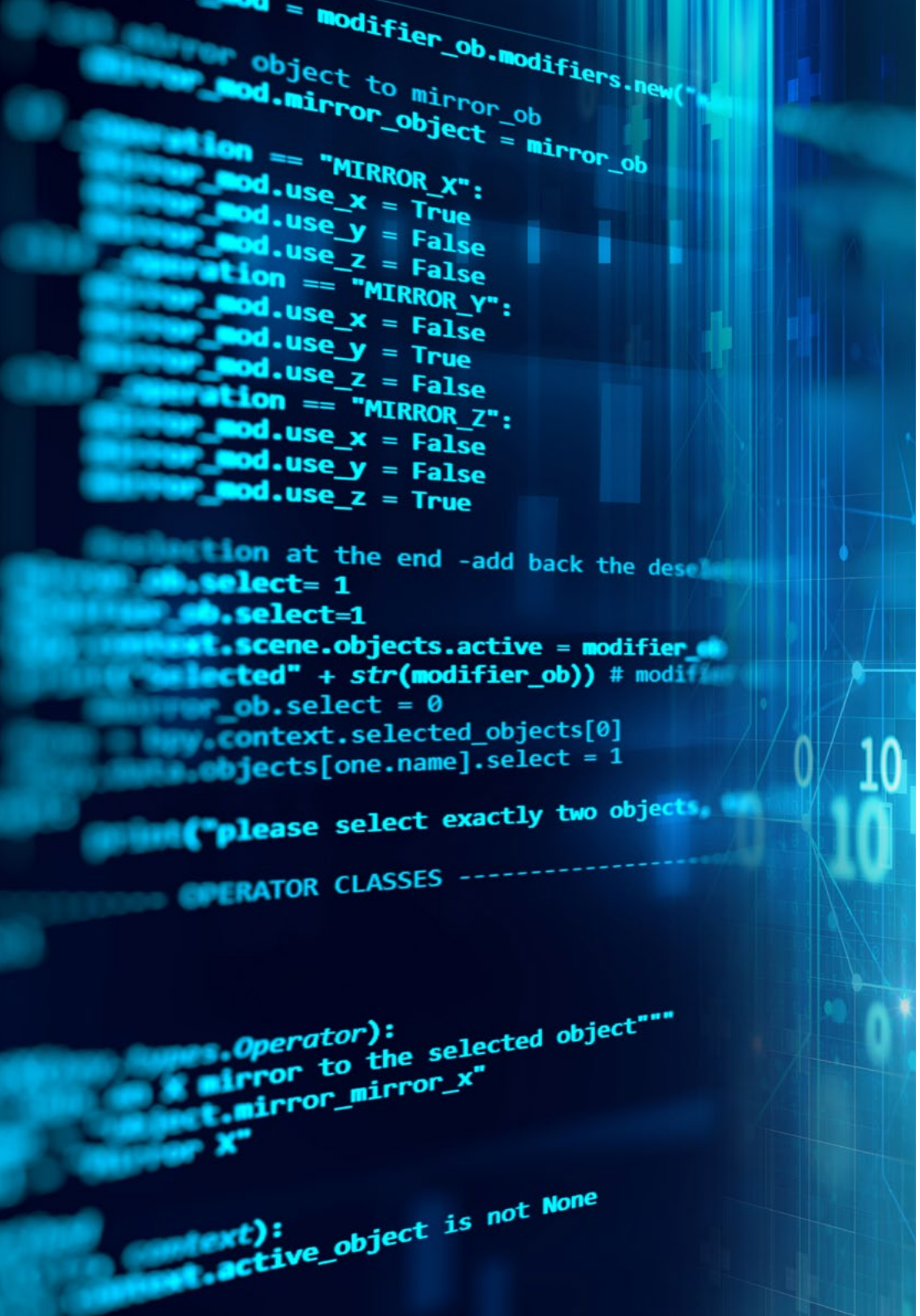
سيسمح لك برنامج الخبرة الجامعية المتاح 100٪ على الإنترنت بدمج دراستك مع عملك المهني. أنت تختار أين ومتى تتدرب.

02

الأهداف

تهدف شهادة الخبرة الجامعية في أمن الحاسوب للاتصالات إلى تسهيل أعمال المتخصصين في هذا المجال حتى يكتسبوا ويتعرفوا على التطورات الرئيسية في هذا المجال.

هدفنا هو أن تصبح أفضل مهني في قطاعك. لهذا لدينا أفضل منهجية ومحتوى"



الهدف العام

- تدريب الطالب على أن يكون قادراً على العمل بأمان وحودة تامة في محال أمن الحاسب الآلي للاتصالات

تدرب في الجامعة الخاصة الرائدة على الإنترنت
الناطقة باللغة الإسبانية الرئيسية في العالم"

الأهداف المحددة

الوحدة 1. الأمن في أنظمة وشبكات الاتصالات

- معرفة ومعرفة كيفية تطبيق أساسيات البرمجة في الشبكات والأنظمة وخدمات الاتصالات
- إتقان المعايير واللوائح الخاصة بالبروتوكولات والشبكات الخاصة بهيئات التقييس الدولية
- فهم مفاهيم التشفير المتماثل وغير المتماثل، والتوقيع الرقمي، ودوال التحزئة، وتأمين كل مستوى من مستويات بنية الاتصالات
- فهم آليات وبروتوكولات الأمان المختلفة القائمة على التحكم في الوصول: المصادقة والدفاع المحيط
- فهم عمل التهديدات التقنية والبشرية لأمن شبكات وأنظمة الاتصالات
- تصنيف خدمات الأمان المختلفة للشبكات والأنظمة بشكل مناسب وفقاً للأصول التي تحميها
- تطبيق أنظمة إدارة الشبكات والخدمات لتهيئة شبكات وخدمات الاتصالات وتشغيلها ومراقبتها وشحنها
- معرفة كيفية إدارة أمن شبكات وخدمات الاتصالات السلكية واللاسلكية من خلال تنفيذ الأنفاق، وحدران الحماية، وبروتوكولات التشفير والمصادقة، وآليات حماية المحتوى
- القدرة على فهم وتطبيق التقنيات الرئيسية للبرمجة الآمنة

الوحدة 2. معماريات الأمن

- فهم المبادئ الأساسية لأمن الكمبيوتر
- إتقان معايير أمن تكنولوجيا المعلومات وعمليات الاعتماد
- تحليل الأسس التنظيمية والتشفيرية التي تستند إليها التقنيات الأمنية
- تحديد التهديدات ونقاط الضعف الرئيسية للعناصر المختلفة التي تنطوي عليها تكنولوجيا المعلومات والاتصالات، وكذلك أسبابها
- معرفة متعمقة بأدوات أمن الشبكات ووظائفها المحددة
- معرفة كيفية تطبيق التقنيات التي تشكل بنية أمن تكنولوجيا المعلومات والاتصالات من مختلف حوانبها

الوحدة 3. تدقيق نظم المعلومات

- إتقان المفاهيم والمعايير والمنهجيات الرئيسية لتدقيق النظم
- دراية بالعناصر التنظيمية والإطار القانوني لعمليات التدقيق
- الحصول على دليل مرجعي لتصميم أنظمة الرقابة الداخلية الحديدة لتكنولوجيا المعلومات
- فهم وتحديد المخاطر المرتبطة بالتطور التكنولوجي وتحديدها
- الكشف عن كيفية تلبية أو عدم تلبية أنظمة المعلومات المختلفة للمتطلبات الأمنية المطلوبة
- القدرة على تنفيذ عملية التحسين المستمر للأمن السيبراني

03

الهيكل والمحتوى

تم تصميم هيكل المحتويات من قبل أفضل المهنيين في قطاع هندسة الاتصالات، ذوي المسيرة المهنية الطويلة والمكانة المعترف بها في المهنة.

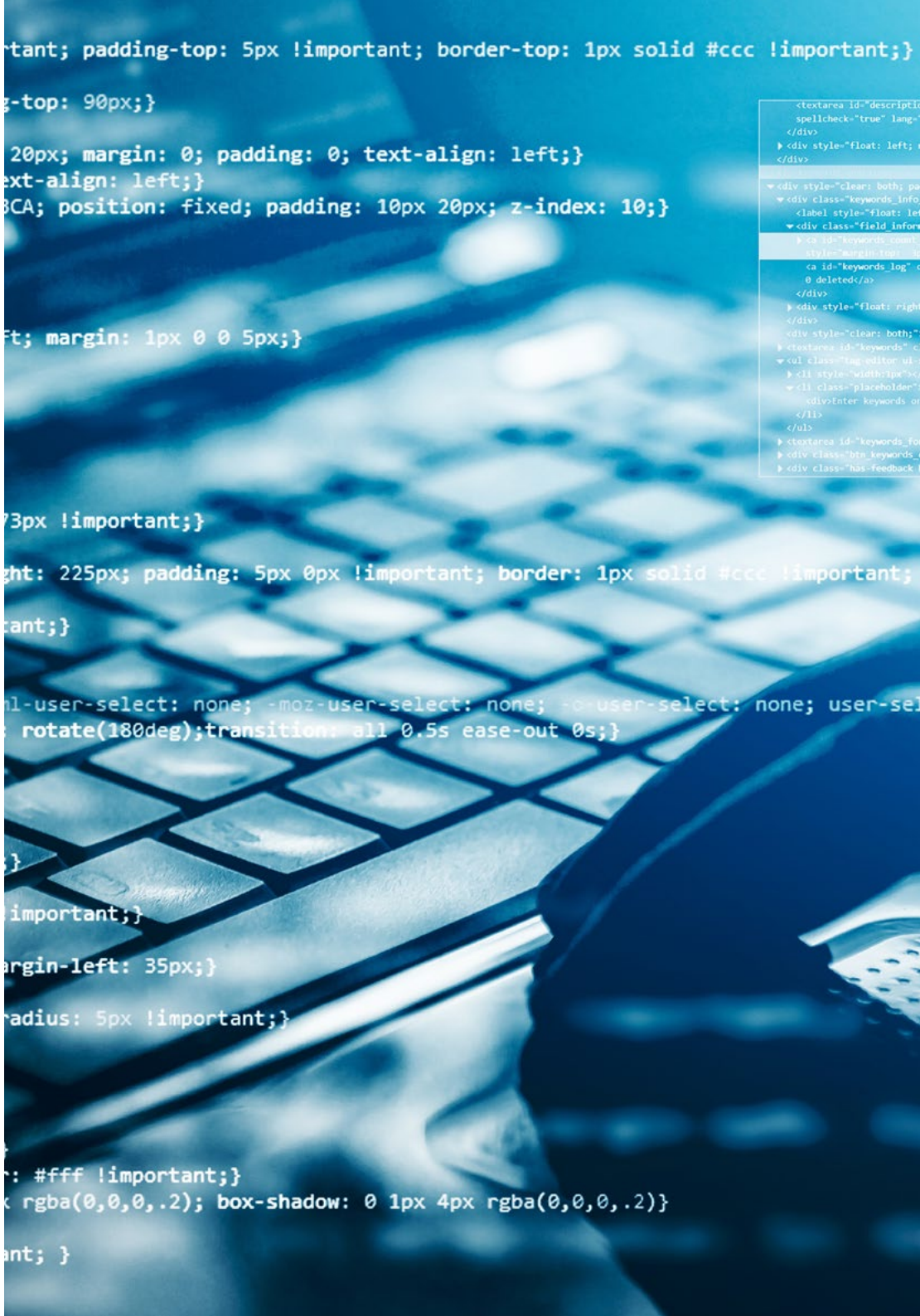
لدينا البرنامج العلمي الأكثر اكتمالا وتحديثا في السوق. نسعى لتحقيقه التميز ولأن تحققه أنت أيضًا"

الوحدة 1. الأمن في أنظمة وشبكات الاتصالات

1.1. منظور عالمي للأمن والتشفير وتحليل الشفرات الكلاسيكي
1.1.1. أمن الحاسوب: منظور تاريخي
2.1.1. لكن ما المقصود بالأمن بالضبط؟
3.1.1. تاريخ علم التشفير
4.1.1. شفرات بديلة
5.1.1. دراسة حالة: آلة إنجما
2.1. التشفير المتماثل
1.2.1. المقدمة والمصطلحات الأساسية
2.2.1. تشفير متماثل
3.2.1. أوضاع التشغيل
4.2.1. DES
5.2.1. معيار AES الجديد
6.2.1. تشفير التدفق
7.2.1. تحليل الشفرات
3.1. التشفير غير المتماثل
1.3.1. أصول التشفير بالمفتاح العام
2.3.1. المفاهيم الأساسية والتشغيل
3.3.1. الخوارزمية RSA
4.3.1. شهادات رقمية
5.3.1. التخزين وإدارة المفاتيح
4.1. هجمات الشبكة
1.4.1. تهديدات وهجمات من شبكة
2.4.1. تعداد
3.4.1. اعتراض حركة المرور: *sniffers*
4.4.1. هجمات رفض الخدمة
5.4.1. هجمات تسمم ARP

5.1. معماريات الأمن
1.5.1. معماريات الأمن التقليدية
2.5.1. SSL: *Secure Socket Layer*
3.5.1. بروتوكول SSH
4.5.1. الشبكات الخاصة الافتراضية (VPN)
5.5.1. آليات الحماية لوحدات التخزين الخارجية
6.5.1. آليات حماية الأجهزة
6.1. تقنيات حماية الأنظمة وتطوير الكود الآمن
1.6.1. السلامة في العمليات
2.6.1. الموارد والضوابط
3.6.1. المراقبة
4.6.1. أنظمة الكشف عن التسلل
5.6.1. المضيف IDS
6.6.1. شبكة IDS
7.6.1. IDS استناداً إلى التوقيعات
8.6.1. أنظمة الشرك
9.6.1. مبادئ الأمان الأساسية في تطوير الاكواد
10.6.1. إدارة الإخفاق
11.6.1. العدو العام رقم 1: تجاوز سعة المخزن المؤقت
12.6.1. أخطاء التشفير
7.1. شبكات الروبوت والبريد المزعج
1.7.1. أصل المشكلة
2.7.1. عملية الرسائل غير المرغوب فيها
3.7.1. إرسال الرسائل غير المرغوب فيها
4.7.1. تنقيح القوائم البريدية
5.7.1. تقنيات الحماية
6.7.1. خدمة مكافحة البريد المزعج التي تقدمها أطراف أخرى
7.7.1. حالات الدراسة
8.7.1. الرسائل غير المرغوب فيها الغريبة

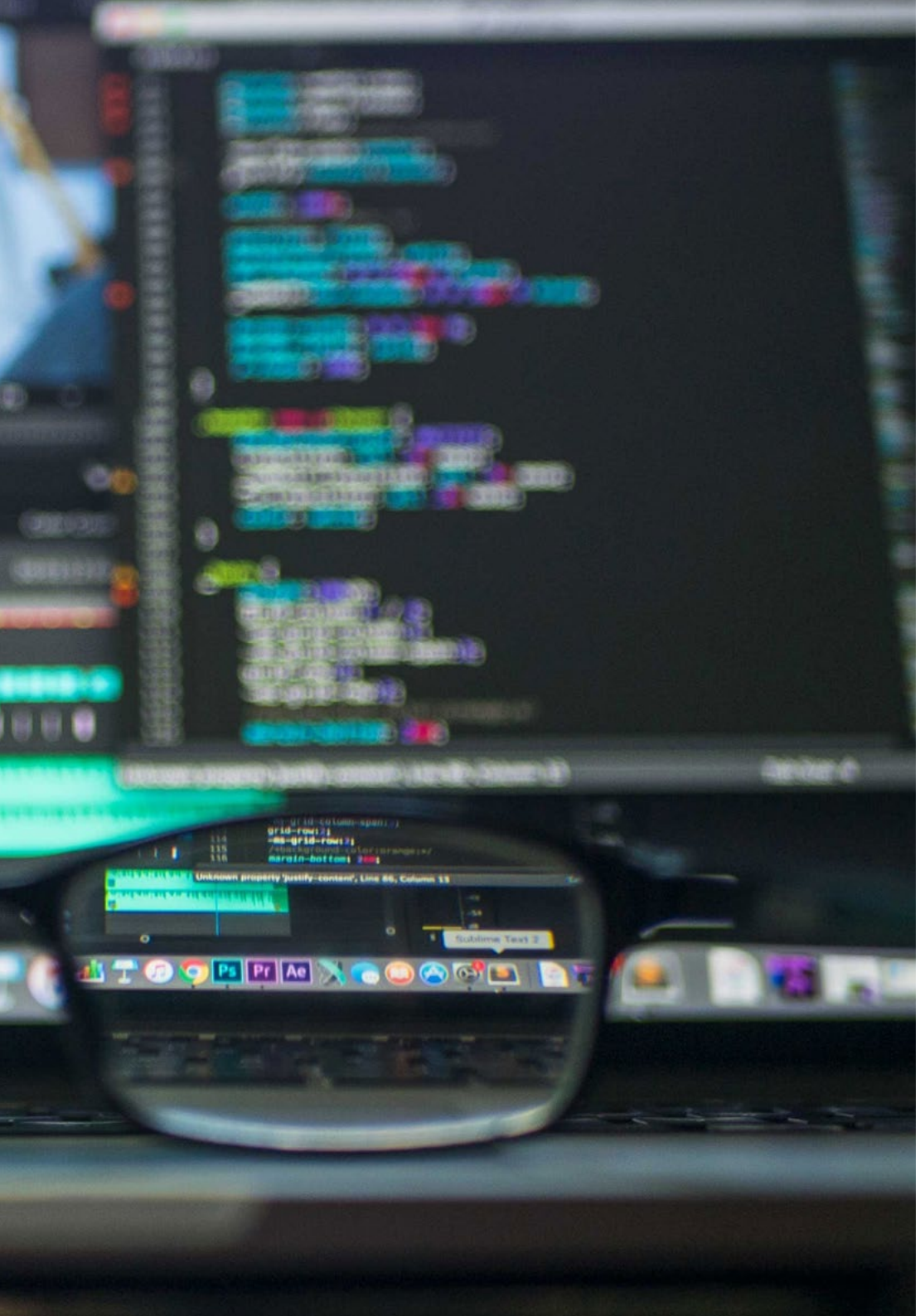
8.1. المراجعة وهجمات الويب
1.8.1. جمع المعلومات
2.8.1. تقنيات الهجوم
3.8.1. الأدوات
9.1. البرمجيات الخبيثة والشفرات الخبيثة
1.9.1. ما هي البرمجيات الخبيثة؟
2.9.1. أنواع البرمجيات الخبيثة
3.9.1. الفيروسات
4.9.1. فيروس مشفر
5.9.1. الديدان
6.9.1. تجسس
7.9.1. *Spyware*
8.9.1. *Hoaxes*
9.9.1. *Pishing*
10.9.1. حصان طروادة
11.9.1. اقتصاد *Malware*
12.9.1. الحلول الممكنة
10.1. التحليل الجنائي
1.10.1. جمع الأدلة
2.10.1. تحليل الأدلة
3.10.1. التقنيات المضادة للطب الشرعي
4.10.1. دراسة حالة عملية



الوحدة 2. معماريات الأمن

1.2. المبادئ الأساسية لسلامة الحوسبة
1.1.2. ما المقصود أمن الحاسبات؟
2.1.2. أهداف أمن تكنولوجيا المعلومات
3.1.2. خدمات أمن تكنولوجيا المعلومات
4.1.2. عواقب انعدام الأمن
5.1.2. مبدأ "الدفاع في الأمن
6.1.2. السياسات والخطط والإجراءات الأمنية
1.6.1.2. إدارة حسابات المستعملين
2.6.1.2. تحديد هوية المستخدم والمصادقة
3.6.1.2. التفويض والتحكم في الوصول المنطقي
4.6.1.2. مراقبة الخادم
5.6.1.2. حماية بيانات
6.6.1.2. الأمن في الاتصالات عن بُعد
7.1.2. أهمية العامل البشري
2.2. توحيد معايير أمن تكنولوجيا المعلومات وإصدار الشهادات
1.2.2. معايير الأمان
1.1.2.2. الغرض من المعايير
2.1.2.2. الهيئات المسؤولة
2.2.2. معايير الولايات المتحدة
1.2.2.2. TCSEC
2.2.2.2. المعايير الفيدرالية
3.2.2.2. FISCAM
4.2.2.2. NIST SP 008
3.2.2. المعايير الأوروبية
1.3.2.2. ITSEC
2.3.2.2. ITSEM
3.3.2.2. الوكالة الأوروبية لأمن الشبكات والمعلومات
4.2.2. المعايير الدولية
5.2.2. عملية الاعتماد
3.2. تهديدات أمن الحاسوب: نقاط الضعف و*Malware*
1.3.2. المقدمة
2.3.2. نقاط الضعف في الأنظمة
1.2.3.2. حوادث أمن الشبكة
2.2.3.2. أسباب ثغرات نظام تكنولوجيا المعلومات
3.2.3.2. أنواع الثغرات الأمنية
4.2.3.2. مسؤوليات مصنعي البرمجيات
5.2.3.2. أدوات تقييم الثغرات الأمنية
3.3.2. تهديدات أمن تكنولوجيا المعلومات
1.3.3.2. تصنيف المتسللين في الشبكات
2.3.3.2. دوافع المهاجمين
3.3.3.2. مراحل الهجوم
4.3.3.2. أنواع الهجمات
4.3.2. فيروسات الحاسب
1.4.3.2. الخصائص العامة
2.4.3.2. أنواع الفيروسات
3.4.3.2. الأضرار التي تسببها الفيروسات
4.4.3.2. كيفية مكافحة الفيروسات
4.2. الإرهاب الإلكتروني والاستجابة للحوادث
1.4.2. المقدمة
2.4.2. تهديد الإرهاب الإلكتروني والحرب الإلكترونية
3.4.2. عواقب الفشل والهجمات على الأعمال التجارية
4.4.2. التجسس على شبكات الكمبيوتر
5.2. أنظمة تحديد هوية المستخدم والقياسات الحيوية
1.5.2. مقدمة في مصادقة المستخدم، والتفويض والتسجيل
2.5.2. نموذج أمان AAA
3.5.2. التحكم في الوصول
4.5.2. تحديد هوية المستخدم
5.5.2. التحقق من كلمة المرور
6.5.2. المصادقة باستخدام الشهادات الرقمية
7.5.2. تحديد هوية المستخدم عن بُعد

8.5.2. تسجيل دخول واحد
9.5.2. مديرى كلمات المرور
10.5.2. أنظمة القياسات الحيوية
1.10.5.2. الخصائص العامة
2.10.5.2. أنواع أنظمة القياسات الحيوية
3.10.5.2. تنفيذ الأنظمة
6.2. أساسيات علم التشفير وبروتوكولات التشفير
1.6.2. مقدمة في التشفير
1.1.6.2. التشفير وتحليل الشفرات والتشفير وعلم التشفير
2.1.6.2. تشغيل نظام التشفير
3.1.6.2. تاريخ أنظمة التشفير
2.6.2. تحليل الشفرات
3.6.2. تصنيف أنظمة التشفير
4.6.2. أنظمة التشفير المتماثل وغير المتماثل
5.6.2. التوثيق باستخدام أنظمة التشفير
6.6.2. التوقيع الالكتروني
1.6.6.2. ما هو التوقيع الإلكتروني؟
2.6.6.2. خصائص التوقيع الإلكتروني
3.6.6.2. سلطات التصديق
4.6.6.2. شهادات رقمية
5.6.6.2. أنظمة قائمة على طرف ثالث موثوق به
6.6.6.2. استخدام التوقيعات الإلكترونية
7.6.6.2. الهوية الإلكترونية
8.6.6.2. الفاتورة الإلكترونية
7.2. أدوات أمان الشبكة
1.7.2. مشكلة أمان الاتصال بالإنترنت
2.7.2. الأمن في الشبكة الخارجية
3.7.2. دور الخوادم الوكيلة Proxy
4.7.2. دور جدران الحماية
5.7.2. خوادم المصادقة للاتصالات عن بُعد
6.7.2. تحليل سجلات الأنشطة
7.7.2. أنظمة الكشف عن التسلل
8.7.2. الشراك الخداعية
8.2. أمان الشبكة اللاسلكية والشبكة الخاصة الافتراضية
1.8.2. أمان الشبكة الخاصة الافتراضية
1.1.8.2 دور الشبكات الافتراضية الخاصة
2.1.8.2 بروتوكولات VPN
2.8.2. أمان الشبكة اللاسلكية التقليدية
3.8.2. الهجمات المحتملة على الشبكات اللاسلكية
4.8.2. بروتوكول WEP
5.8.2. معايير أمان الشبكة اللاسلكية
6.8.2. توصيات لتعزيز الأمن
9.2. السلامة في استخدام خدمات الإنترنت
1.9.2. التصفح الآمن للويب
1.1.9.2. خدمة www
2.1.9.2. مشاكل أمنية في www
3.1.9.2. توصيات السلامة
4.1.9.2. حماية الخصوصية على الإنترنت
2.9.2. أمان البريد الإلكتروني
1.2.9.2. خصائص البريد الإلكتروني
2.2.9.2. مشكلات أمان البريد الإلكتروني
3.2.9.2. توصيات أمان البريد الإلكتروني
4.2.9.2. خدمات البريد الإلكتروني المتقدمة
5.2.9.2. استخدام البريد الإلكتروني من قبل الموظفين
3.9.2. الرسائل غير المرغوب فيها
4.9.2. *phising*
10.2. التحكم في المحتوى
1.10.2. توزيع المحتوى عبر الإنترنت
2.10.2. التدابير القانونية لمكافحة المحتوى غير القانوني
3.10.2. تصفية المحتوى وفهرسته وحظره
4.10.2. الإضرار بالصورة والسمعة



الوحدة 3. التدقيق انظمة المعلومات

1.3. التدقيق نظم المعلومات. معايير الممارسة الجيدة
1.1.3. المقدمة
2.1.3. التدقيق و COBIT
3.1.3. مراجعة أنظمة إدارة تكنولوجيا المعلومات والاتصالات TIC
4.1.3. الشهادات:
2.3. مفاهيم ومنهجيات تدقيق النظم
1.2.3. المقدمة
2.2.3. منهجيات تقييم النظام: الكمية والنوعية
3.2.3. منهجيات تدقيق تكنولوجيا المعلومات
4.2.3. خطة التدقيق
3.3. عقد التدقيق
1.3.3. الطبيعة القانونية للعقد
2.3.3. أطراف عقد التدقيق
3.3.3. موضوع عقد المراجعة
4.3.3. تقرير التدقيق
4.3. العناصر التنظيمية لعمليات مراجعة الحسابات
1.4.3. المقدمة
2.4.3. مهمة قسم مراجعة الحسابات
3.4.3. تخطيط التدقيق
4.4.3. منهجية مراجعة الحسابات لنظام SI
5.3. الإطار القانوني لعمليات التدقيق
1.5.3. حماية البيانات الشخصية
2.5.3. الحماية القانونية للبرمجيات
3.5.3. الجرائم التكنولوجية
4.5.3. التوظيف والتوقيع والهوية الإلكترونية
6.3. الاستعانة بـ*Outsourcing* للتدقيق الخارجي وأطر العمل
1.6.3. المقدمة
2.6.3. أساسيات *Outsourcing*
3.6.3. تدقيق الاستعانة بـ*Outsourcing* لتكنولوجيا المعلومات
4.6.3. الإطار المرجعي ISO، CMMI، 10072، ITIL

7.3. التدقيق الأمني
1.7.3. المقدمة
2.7.3. الأمن المادي والمنطقي
3.7.3. أمن البيئة
4.7.3. التخطيط لمراجعة الأمن المادي وتنفيذها
8.3. التدقيق الشبكة والإنترنت
1.8.3. المقدمة
2.8.3. نقاط ضعف الشبكة
3.8.3. المبادئ والحقوق على الإنترنت
4.8.3. الضوابط ومعالجة البيانات
9.3. تدقيق تطبيقات وأنظمة تكنولوجيا المعلومات
1.9.3. المقدمة
2.9.3. النموذج المرجعي
3.9.3. تقييم جودة الطلبات
4.9.3. مراجعة تنظيم وإدارة منطقة التطوير والصيانة وإدارتها
10.3. تدقيق البيانات الشخصية
1.10.3. المقدمة
2.10.3. قوانين ولوائح حماية البيانات
3.10.3. تطوير مراجعة الحسابات
4.10.3. المخالفات والعقوبات

سيسمح لك هذا التدريب بالتقدم
في حياتك المهنية بطريقة مريحة"

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.

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.

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

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.

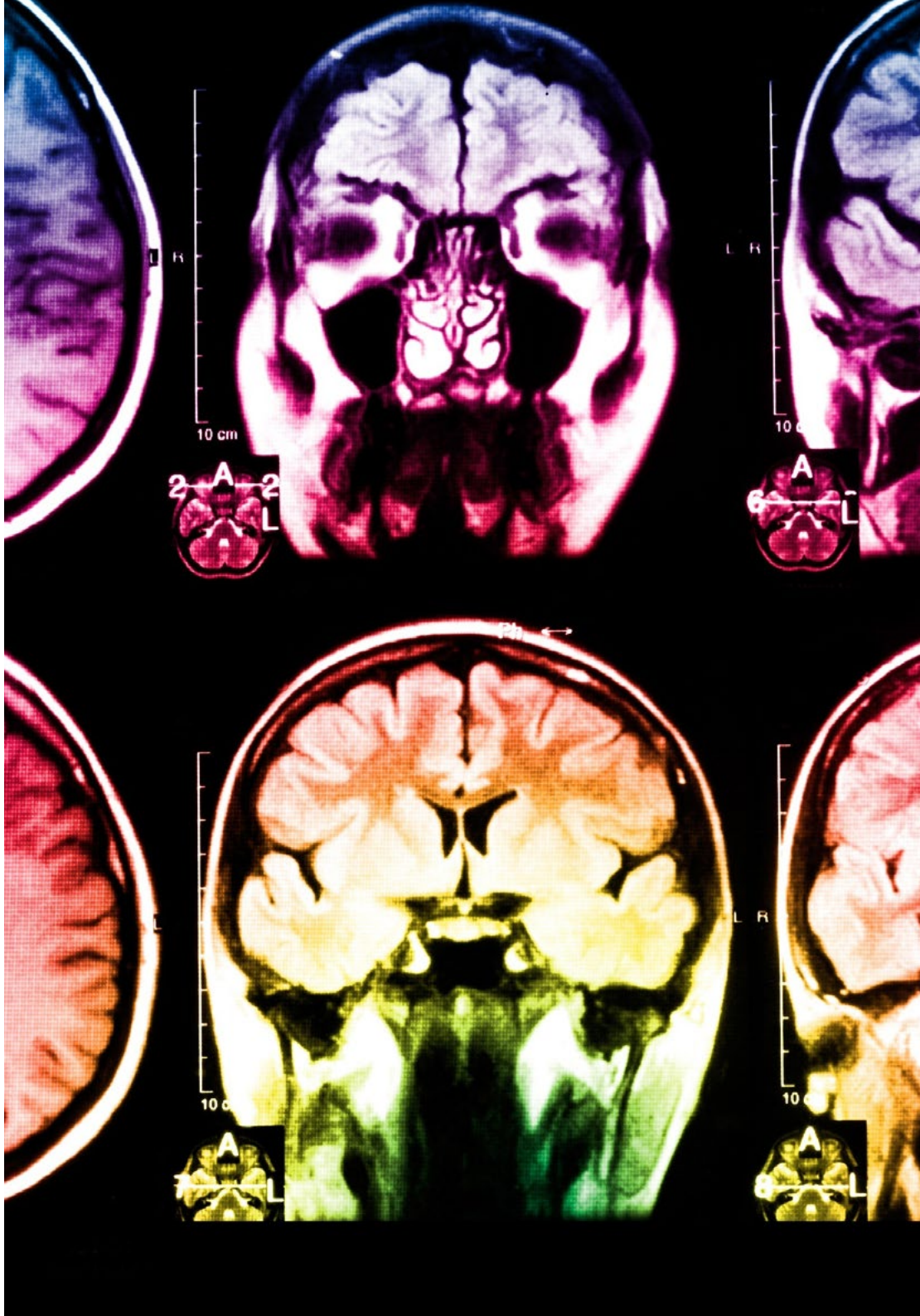
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

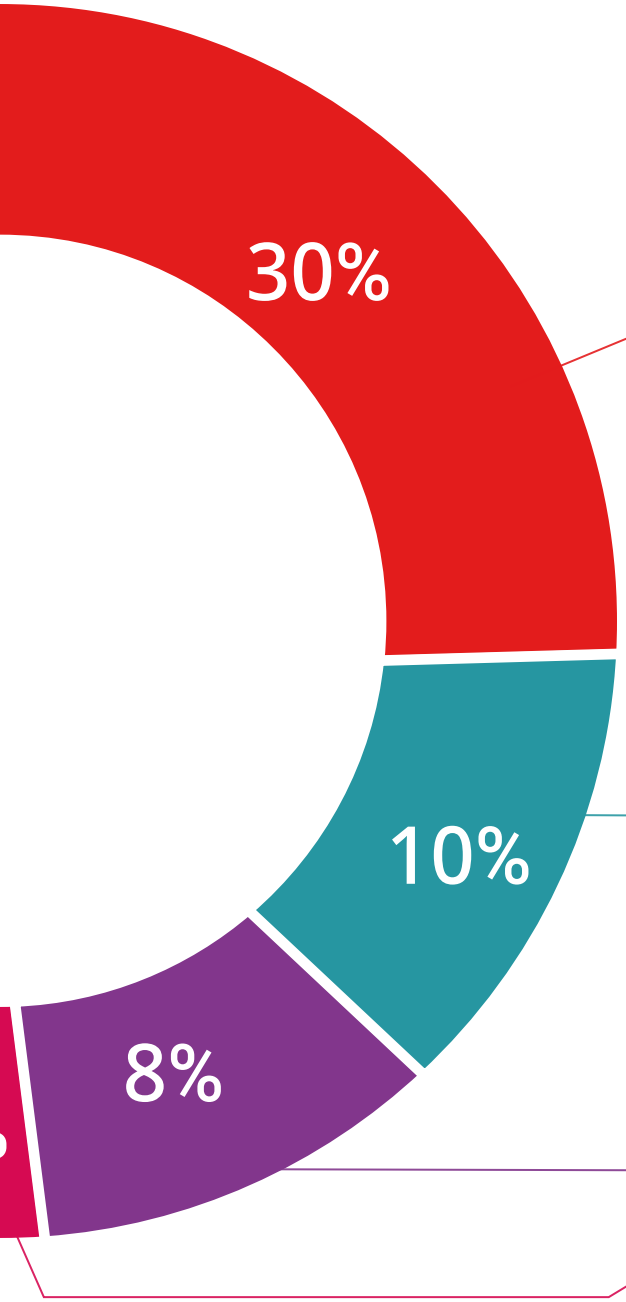
في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلّم ثم نطرح ماتعلمناه جانبًا فننساه ثم نعيد تعلمه). لذلك، نقوم بدمج كل عنصر من هذه العناصر بشكل مركزي. باستخدام هذه المنهجية، تم تدريب أكثر من 650000 خريج جامعي بنجاح غير مسبوق في مجالات متنوعة مثل الكيمياء الحيوية، وعلم الوراثة، والجراحة، 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.

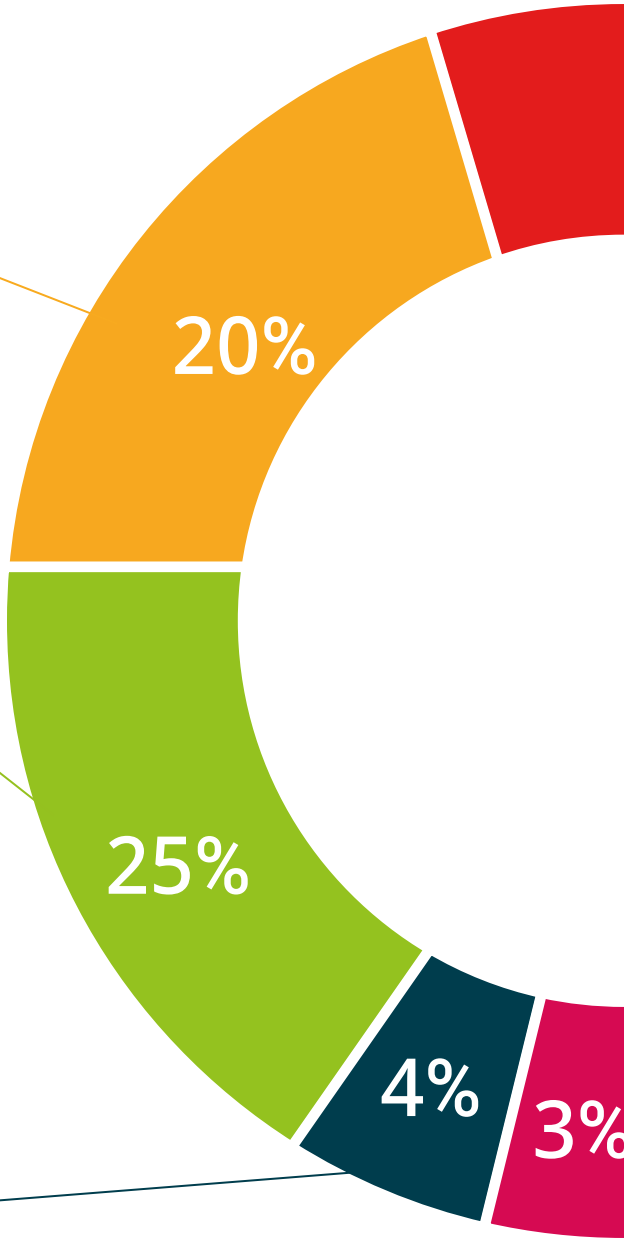
ملخصات تفاعلية

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

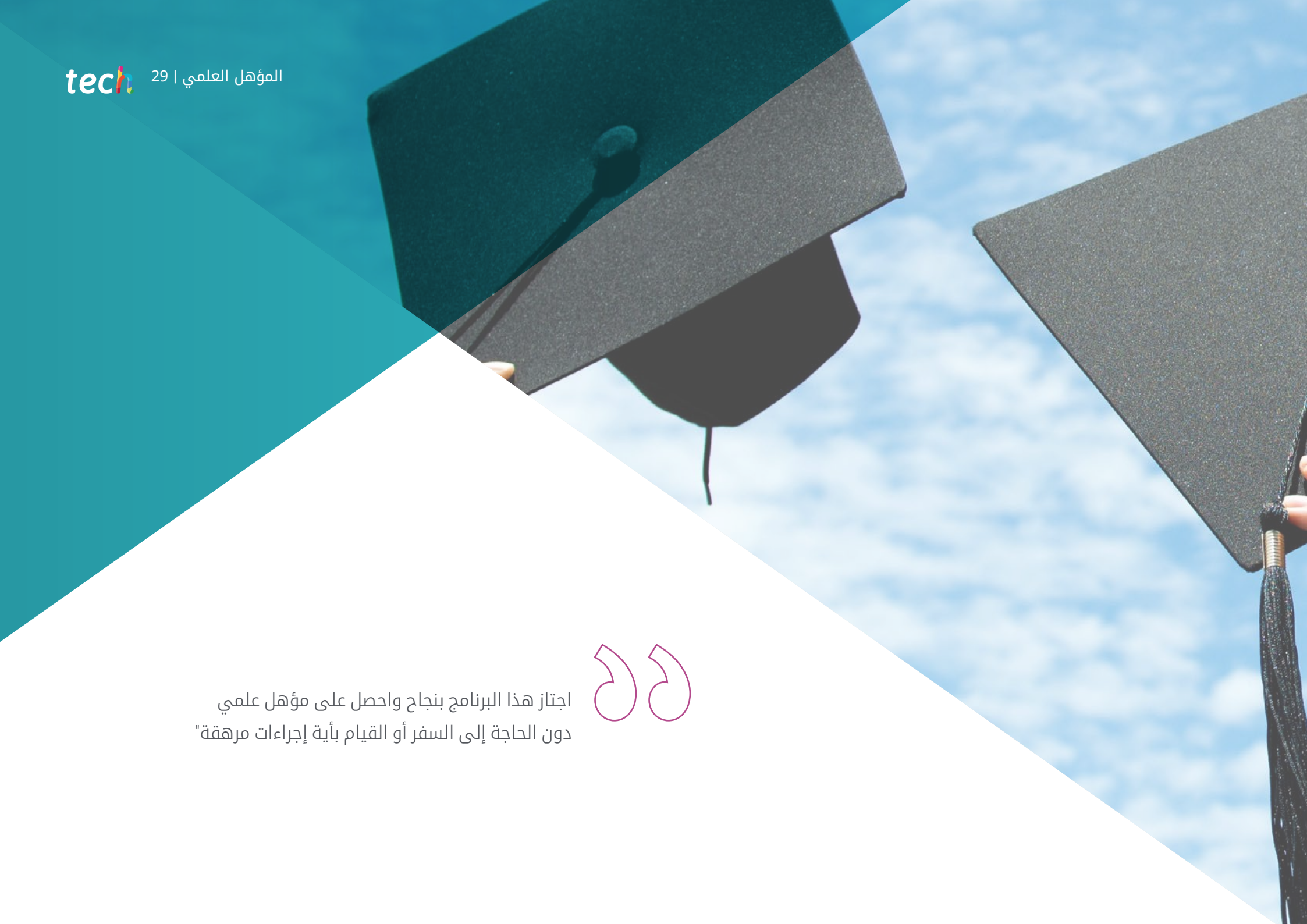
يتم بشكل دوري تقييم وإعادة تقييم معرفة الطالب في جميع مراحل البرنامج، من خلال الأنشطة والتدريبات التقييمية وذاتية التقييم: حتى يتمكن من التحقق من كيفية تحقيق أهدافه.



05

المؤهل العلمي

تضمن شهادة الخبرة الجامعية في أمن الحاسوب للاتصالات، بالإضافة إلى التدريب الأكثر دقة وحداثة، الحصول على مؤهل شهادة الخبرة الجامعية الصادر عن TECH الجامعة التكنولوجية.



اجتاز هذا البرنامج بنجاح واحصل على مؤهل علمي
دون الحاجة إلى السفر أو القيام بأية إجراءات مرهقة"

تحتوي ال **شهادة الخبرة الجامعية في أمن الحاسوب للاتصالات** على البرنامج العلمية الأكثر اكتمالا و حداثة في السوق.

بعد اجتياز التقييم، سيحصل الطالب عن طريق البريد العادي* مصحوب بعلم وصول مؤهل ال **محاضرة الجامعية** الصادرعن **TECH الجامعة التكنولوجية.**

إن المؤهل الصادرعن **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: **شهادة الخبرة الجامعية في أمن الحاسوب للاتصالات**

طريقة: **عبر الإنترنت**

مدة: **6 اشهر**


tech الجامعة التكنولوجية

شهادة تخرج

هذه الشهادة ممنوحة إلى

لـ

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

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

شهادة الخبرة الجامعية

في

أمن الحاسوب للاتصالات

وهي شهادة خاصة من هذه الجامعة موافقة لـ 450
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.

tech الجامعة التيكنولوجية

شهادة الخبرة الجامعية

أمن الحاسوب للاتصالات

- طريقة التدريس: **أونلاين**
- مدة الدراسة: **6 اشهر**
- المؤهل الجامعي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **أونلاين**

شهادة الخبرة الجامعية
أمن الحاسوب للاتصالات

tech الجامعة التيكنولوجية