ماجيستير خاص
MBA إدارة الأمن الإلكترونى
(CISO, Chief Information Security Officer)

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

ماجيستير خاص
MBA إدارة الأمن الإلكترونى
(CISO, Chief Information Security Officer)

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

رابط الدخول إلى الموقع الإلكترونى: **www.techtitute.com/ae/school-of-business/executive-master-degree/master-cybersecurity-management-ciso-chief-information-security-officer**

الفهرس

01

كلمة الترحيب

مجتمع اليوم مترابط بشكل مفرط. عصر المعلومات يسمح للمواطنين بأن يكونوا على علم بأي بيانات بنقرة واحدة فقط. ولكن هذا تسبب أيضًا في أن تصبح التهديدات الافتراضية هي واقع الوضع الحالى، لذا أصبحت الشركات أكثر عرضة من أي وقت مضى لتلقي software ضار يلحق الضرر بإنتاجها وأمنها، وحتى تعرض البيانات الشخصية للعملاء والعاملين للخطر، وهذا يكشف نقاط الضعف في تكنولوجيا المعلومات لديهم. على الرغم من أن الحماية في هذا المجال هي مهمة مهندسى البرمجة، إلا أن المزيد والمزيد من chief revenue officers وغيرهم من المديرين يقررون التخصص في هذا المجال لمحاولة إيقاف مجرمي الإنترنت وتجنب أن يكونوا هدفًا لهجماتهم. لهذا السبب، أنشأت TECH هذا البرنامج، حيث سيجد محترفوا الأعمال المعلومات الأكثر صلة بالوضع الحالى، من خلال منهج تعليمي سيكون من السهل فهمه للطلاب. وبالتالي، وبفضل المعرفة المكتسبة، سيكون الخريج قادرًا على العمل بنجاح كمديرامن المعلومات، وهو منصب آخذ في الارتفاع مع آفاق نمو كبيرة.

MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer)
TECH الجامعة التكنولوجية

عزز مهاراتك فى إدارة أعمال الأمن الإلكترونية بفضل 10 فصول رئيسية حصرية من قبل متخصص مشهور عالميًا فى هذا المجال"

02

لماذا تدرس في TECH؟

إن جامعة TECH هي أكبر كلية إدارة أعمال في العالم 100٪ عبر الإنترنت. إنها مدرسة إدراة أعمال النخبة، ذات نموذج الحد الأقصى من المتطلبات الأكاديمية. ومركز دولي عالي الأداء، يتمتع بتدريب مكثف على المهارات الإدارية.

جامعة TECH هي جامعة تكنولوجية رائدة، تضع جميع مصادرها في متناول الطلاب لمساعدتهم على تحقيق النجاح في إدارة الأعمال"

في TECH الجامعة التكنولوجية

الابتكار

تقدم لك الجامعة نموذجًا تعليميًا عبر الإنترنت يجمع بين أحدث التقنيات التعليمية وأعلى دقة تربوية.
إنه منهج فريد من نوعه يتمتع بأكبر قدر من الاعتراف الدولي والذي سيوفر للطالب مفاتيح التطور في عالم يتغير باستمرار، حيث يجب أن يكون الابتكار هو الرهان الأساسي لكل رائد أعمال.

"قصة نجاح Microsoft Europe" وذلك لدمج نظام الفيديو التفاعلي الجديد في البرامج.

أعلى المعايير

معايير القبول جامعة TECH ليست مادية. ليس هناك حاجة إلى القيام باستثمار كبير للدراسة معنا. بالطبع، من أجل الحصول على مؤهل من TECH الجامعة التكنولوجية، سيتم اختبار ذكاء الطالب وقدرته إلى أقصى حدوده.
المعايير الأكاديمية للمؤسسة عالية بشكل استثنائي..

95% | من طلاب جامعة TECH يكملون دراساتهم بنجاح.

إقامة شبكة جيدة من العلاقات

يشارك المحترفون من جميع أنحاء العالم في جامعة TECH، بطريقة يمكن للطالب من خلالها إنشاء شبكة كبيرة من الاتصالات المفيدة لمستقبله.

+100.000
مدراء تنفيذيون يتم تدريبهم كل سنة

+200
جنسية مختلفة

التمكين

سينمو الطالب جنبًا إلى جنب مع أفضل الشركات والمهنيين ذوي المكانة والتأثير الكبير.
طورت جامعة TECH تحالفات استراتيجية وشبكة قيمة من الاتصالات مع الممثلين الاقتصاديين الرئيسيين في القارات السبع.

+500 | اتفاقية تعاون مع أفضل الشركات

الموهبة

هذا البرنامج هو عرض فريد لإبراز موهبة الطالب في مجال الأعمال. إنها فرصة يمكنه من خلالها التعريف بمخاوفه ورؤية عمله.

تساعد جامعة TECH الطالب على إظهار موهبته للعالم في نهاية هذا البرنامج.

سياق متعدد الثقافات

عند الدراسة في جامعة TECH، سيتمكن الطالب من الاستمتاع بتجربة فريدة من نوعها. سوف يدرس في سياق متعدد الثقافات. في برنامج ذي رؤية عالمية، سيتمكن بفضله من تعلم كيفية العمل في أنحاء مختلفة من العالم، وتجميع أحدث المعلومات التي تناسب فكرة عمله.

يأتي طلاب جامعة TECH من أكثر من 200 جنسية.

تسعى جامعة TECH إلى التميز ولهذا لديها سلسلة من الخصائص التي تجعلها جامعة فريدة من نوعها:

التحليلات

في جامعة TECH، يتم استكشاف الجانب النقدي للطالب وقدرته على طرح الأسئلة ومهارات حل المشكلات ومهارات التعامل مع الآخرين.

التميز الأكاديمي

في جامعة TECH يتم توفير أفضل منهجية تعلم عبر الإنترنت للطالب. تجمع الجامعة بين طريقة إعادة التعلم *Relearning* (منهجية التعلم للدراسات العليا صاحبة أفضل تصنيف دولي) مع دراسة الحالة. التقاليد والريادة في توازن صعب، وفي سياق مسار الرحلة الأكاديمية الأكثر تطلبًا.

الإقتصاد الكلي

تعد جامعة TECH أكبر جامعة أونلاين في العالم. فتخر حاليًا بمحفظة تضم أكثر من 10000 برنامج دراسات عليا جامعي. وفي الاقتصاد الجديد، الحجم + التكنولوجيا = سعر مذهل.. بهذه الطريقة، تضمن TECH الجامعة التكنولوجية أن الدراسة ليست باهظة التكلفة للطلاب كما لو كانت في جامعة أخرى.

تعلم مع الأفضل

يشرح فريق تدريس جامعة TECH في الفصل ما أدى إلى النجاح في شركاتهم، والعمل من سياق حقيقي وحيوي وديناميكي. يقدم المعلمون المشاركون بشكل كامل تخصصًا عالي الجودة يسمح بالتقدم في حياته المهنية والتميز في عالم الأعمال.

في جامعة TECH، ستتمكن من الوصول إلى دراسات الحالة الأكثر صرامة وحداثة في المشهد الأكاديمي"

03

لماذا تدرس برنامجنا هذا تحديدًا؟

تعني دراسة برنامج TECH الجامعة التكنولوجية هذا زيادة فرص تحقيق النجاح المهني في إدارة الأعمال العليا.

إنه تحد يتطلب الجهد والتفاني، لكنه يفتح الباب لمستقبل واعد. سيتعلم الطلاب من أفضل أعضاء هيئة التدريس وباستخدام المنهجية التعليمية الأكثر مرونة وابتكارًا.

نحظى بمدرسين مؤهلين تأهيلاً عالياً ومناهج تعليمية كاملة في السوق، مما يتيح لنا أن نقدم لك تدريبًا على أعلى مستوى أكاديمي"

سيوفر هذا البرنامج للطلاب العديد من المزايا المهنية والشخصية، لا سيما ما يلي:

01 إعطاء دفعة أكيدة لمسيرة الطالب المهنية

من خلال الدراسة في TECH الجامعة التكنولوجية، سيتمكن الطلاب من التحكم في مستقبلهم وتطوير إمكاناتهم الكاملة. من خلال إكمال هذا البرنامج، سيكتسب الطلاب المهارات المطلوبة لإحداث تغيير إيجابي في حياتهم المهنية في فترة زمنية قصيرة.

70% من المشاركين يحققون تطورًا وظيفيًا إيجابيًا في أقل من عامين.

02 تطوير رؤية استراتيجية وعالمية للشركات

تقدم TECH الجامعة التكنولوجية نظرة عامة متعمقة على الإدارة العامة لفهم كيفية تأثير كل قرار على كل مجال من المجالات الوظيفية المختلفة للشركة.

ستعمل رؤيتنا العالمية للشركات على تحسين رؤيتك الإستراتيجية.

03 تعزيز مهارات الإدارة العليا للطالب

تعني الدراسة في TECH الجامعة التكنولوجية فتح الأبواب أمام مجموعة واسعة من الفرص المهنية للطلاب لوضع أنفسهم كمديرين تنفيذيين كبار، مع رؤية واسعة للبيئة الدولية.

ستعمل على أكثر من 100 قضية إدارية عليا حقيقية.

04 تحمل مسؤوليات جديدة

سيغطي البرنامج أحدث الاتجاهات والتقدم،والاستراتيجيات حتى يتمكن الطلاب من القيام بعملهم المهني في بيئة متغيرة.

45٪ ممن يتم ترقيتهم من الطلاب في وظائفهم من خلال الترقية الداخلية.

05 الوصول إلى شبكة قوية من جهات الاتصال

TECH الجامعة التكنولوجية تربط طلابها لتحقيق أقصى قدر من الفرص. الطلاب الذين لديهم نفس الاهتمامات والرغبة في النمو. لذلك، يمكن مشاركة الشراكات أو العملاء أو الموردين.

ستجد شبكة من الاتصالات ستكون مفيدة للتطوير المهني.

06 تطوير المشاريع التجارية بدقة

سيكتسب الطلاب رؤية إستراتيجية عميقة من شأنها مساعدتهم على تطوير مشروعهم الخاص، مع مراعاة المجالات المختلفة في الشركات.

20٪ من طلابنا يطورون أفكارهم التجارية الخاصة.

07 تحسين المهارات الشخصية والمهارات الإدارية

تساعد جامعة TECH الطالب على تطبيق وتطوير المعرفة المكتسبة وتحسين مهاراتك الشخصية ليصبح قائدًا يُحدث فرقًا.

حسّن مهارات الاتصال والقيادة لديك وامنح حياتك المهنية دفعة قوية للأمام.

08 كن جزءًا من مجتمع حصري

سيكون الطالب جزءًا من مجتمع من نخبة المديرين والشركات الكبيرة والمؤسسات المشهورة والأساتذة المؤهلين من أرقى الجامعات في العالم، مجتمع TECH التكنولوجية.

نحن نمنحك الفرصة للتخصص مع فريق من المعلمين المشهورين دوليًا.

04
الأهداف

تم تصميم برنامج TECH هذا لتعزيز القدرات المهنية لمديري الأعمال، الذين بالإضافة إلى تخصصهم على نطاق واسع في مجال نشاطهم، سيجدون في هذا البرنامج فرصة فريدة للتحسين في كجال ذو أهمية كبيرة، حيث أنهم سوف تعلم كيفية منع تهديدات الإنترنت المحتملة التي يمكن أن تسبب أضرارًا جسيمة للشركات. وبهذه الطريقة، سيصبحون خبراء محترفين في مختلف الفروع، وبالتالي سيكونون قادرين على التحكم في جميع مجالات الشركة، وبالتالي كمدير لأمن المعلومات.

زد تدريبك وحقق أهداف عملك بفضل التدريب
ذات المستوى العالمى الذي تقدمه جامعة
TECH من خلال هذا البرنامج"

تحتضن **TECH** أهداف طلابها
نحن نعمل معاً لتحقيقها

فى الماجستير الخاص فى MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer) سيتم تدريب الطلاب على:

01 تحليل دور المحلل في الأمن السيبراني

02 التعمق في الهندسة الاجتماعية وأساليبه

03 دراسة منهجيات استخبارات المصادر المفتوحة، الاستخبارات البشرية، مشروع أمان تطبيق الويب المفتوح، منصة تكنولوجيا البناء، دليل منهجية اختبار الأمان مفتوح المصدر، منهجية تقييم الأمن اللاسلكي المفتوح

04 إجراء تحليل للمخاطر ومعرفة مقاييس المخاط

05 تحديد الاستخدام الصحيح لإخفاء الهوية واستخدام الشبكات مثل TOR و I2P و Freenet

06 تجميع اللوائح الحالية بشأن الأمن السيبراني

07 خلق المعرفة المتخصصة لإجراء تدقيق أمني

08 تطوير سياسات الاستخدام المناسبة

09 فحص أنظمة الكشف والوقاية من أهم التهديدات

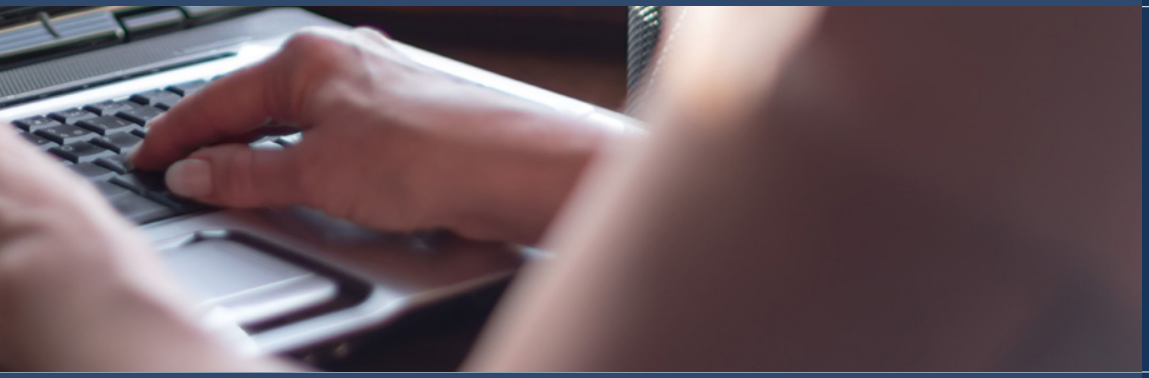
10 تقييم أنظمة الكشف الجديدة عن التهديدات، وكذلك تطورها فيما يتعلق بالحلول الأكثرتقليدية

11 تحليل منصات المحمول الرئيسية الحالية وخصائصها واستخدامه

12 تحديد وتحليل وتقييم المخاطر الأمنية لإجزاء مشروع إنترنت الأشياء

13 تقييم المعلومات التي تم الحصول عليها وتطوير آليات الوقاية والاختراق

14 تطبيق الهندسة العكسية على بيئة الأمن السيبراني



15 تحديد الاختبارات التي يجب إجراؤها على البرنامج المطو

16 جمع كل الأدلة والبيانات الموجودة لإعداد تقرير جنائي

17 تقديم تقرير التحليل الجنائي على النحو الواجب

18 تحليل الحالة الراهنة والمستقبلية لأمن الحاسوب

19 دراسة مخاطر التكنولوجيات الجديدة الناشئة

20 تجميع التكنولوجيات المختلفة فيما يتعلق بأمن الحاسوب

05

الكفاءات

تم تصميم الماجستير الخاص فى MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer) لتحسين القدرة التنافسية للمهنيين في قطاع الأعمال. لذلك، في نهاية دراستهم، سيكون الطلاب قد اكتسبوا المهارات اللازمة لتطوير الجودة والتطبيق العملي المحدث بناءً على منهجية التدريس الأكثر ابتكارًا. إنه بلا شك برنامج سيعمل على تحسين تدريبهم ويسمح لهم بأن يكونوا أكثر قدرة على المنافسة في ممارساتهم اليومية، من خلال توحيد جميع الجوانب ذات الصلة بأمن الحاسوب التي يجب على المديرين معرفتها ووضعها موضع التنفيذ.

تعمق في دراسة أمن الحاسوب وتحسين مهاراتك
للتحكم في تهديدات الشبكة المحتملة"

01 معرفة المنهجيات المستخدمة في مجال الأمن السيبراني

02 معرفة تقييم كل نوع من أنواع التهديد لتقديم الحل الأمثل في كل حالة

03 خلق حلول ذكية كاملة لميكنة سلوكيات الحوادث

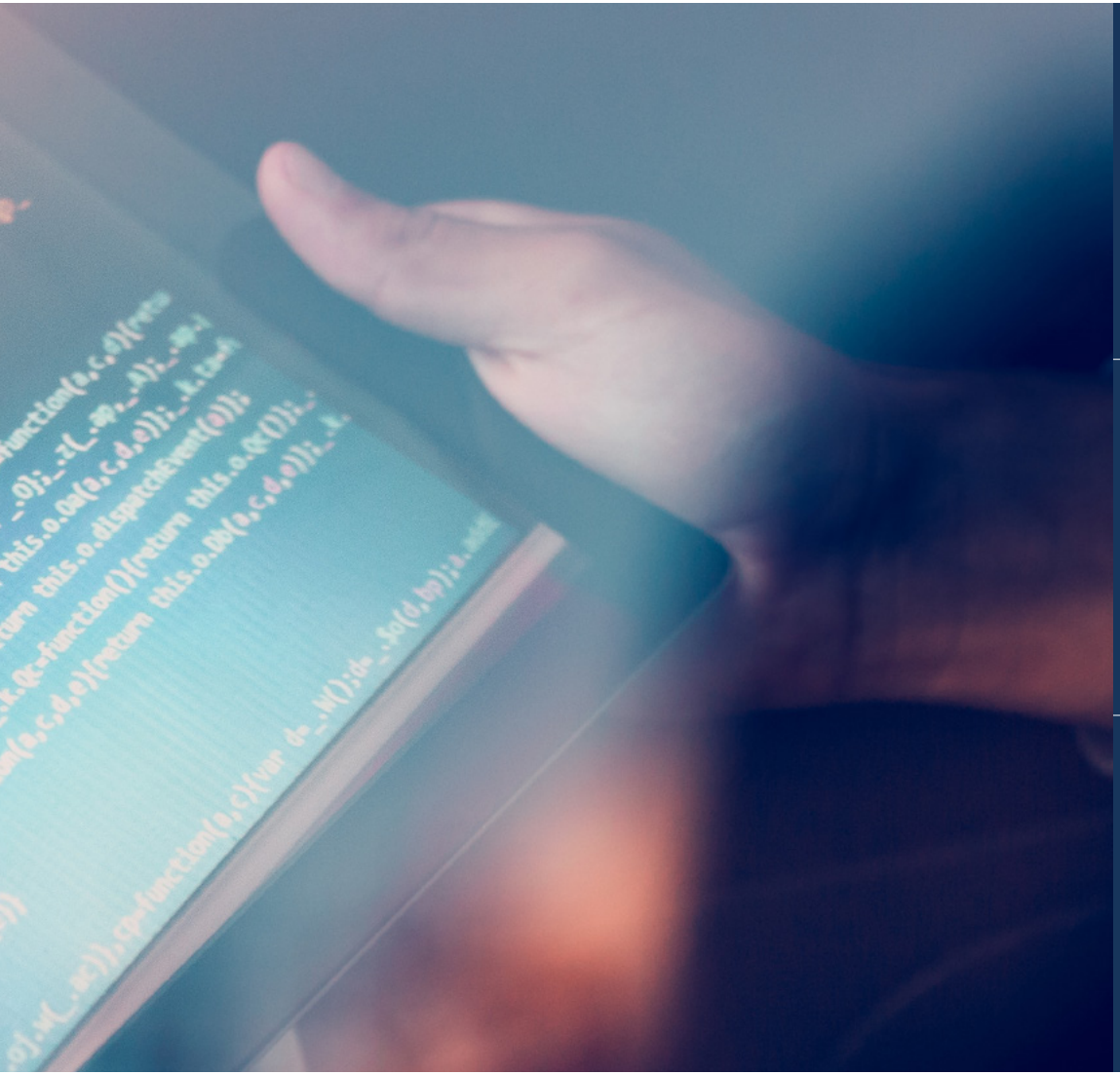
04 تقييم المخاطر المرتبطة بنقاط الضعف خارج الشركة وداخلها على حد سواء

05 التعرف على تطور وتأثير إنترنت الأشياء بمرور الوقت

06 إظهار ضعف النظام، ومهاجمته لأغراض وقائية وحل المشكلات المذكورة

07 معرفة تطبيق sandboxing فى البيئات المختلفة

08 تجديد الإرشادات التي يجب على المطور الجيد اتباعها لتلبية الأمان اللازم



09 التعرف على تنفيذ عمليات الأمن الدفاعية

10 امتلاك تصور عميق ومتخصص لأمن الحاسوب

11 التعرف على تطبيق عمليات الأمان على الهواتف الذكية والأجهزة المحمولة

12 التعرف على وسائل تنفيذ مايسمى Hacking القرصنة الأخلاقية وحماية الشركة من هجوم إلكترونى

13 القدرة على التحقيق في حادث الأمن السيبراني

14 التعرف على تقنيات الهجوم والدفاع المختلفة الموجودة

06

الهيكل والمحتوى

تم تصميم برنامج TECH هذا لتلبية الاحتياجات المتخصصة لمحترفي الأعمال الذين يرغبون في توسيع معرفتهم نحو أمن الحاسوب، وهو مجال أساسي ليكونوا قادرين على التحكم في تلك التهديدات المحتملة التي يمكن أن تشكل خطرًا كبيرًا على الشركة. بهذه الطريقة، ستسمح لهم شهادة MBA باكتساب تلك المعرفة المحددة التي يمكنهم تطبيقها على ممارسة عملهم. لهذا، سيستخدمون منهجية عبر الإنترنت بالكامل تسمح لهم بدمج دراستهم مع بقية التزاماتهم اليومية.

سيكون هذا البرنامج ضروريًا للكشف عن الهجمات الإلكترونية المحتملة على شركتك"

خطة الدراسة

MBA إدارة الأمن السيبراني (CISO، مدير أمن المعلومات) من TECH الجامعة التكنولوجية هو برنامج مكثف مصمم لتعزيز تطوير المهارات الإدارية التي تمكن اتخاذ القرارات بصرامة أكبر في بيئات غير مؤكدة.

طوال 2700 ساعة من الدراسة، سيدرس الطالب العديد من الحالات العملية من خلال العمل الفردي، مما سيسمح له باكتساب المهارات اللازمة للتطور بنجاح في ممارسته اليومية. بالتالي، فهو انغماس حقيقي في مواقف العمل الحقيقية.

يتعامل هذا البرنامج بعمق مع مجالات مختلفة من الشركة وهو مصمم للمديرين لفهم الأمن السيبراني من منظور استراتيجي ودولي ومبتكر.

خطة مصممة خصيصًا للطلاب، وتركز على تحسينهم المهني وإعدادهم لتحقيق التميز في مجال توجيه وإدارة أمن تكنولوجيا المعلومات. برنامج يتفهم احتياجات الطالب واحتياجات شركتك من خلال محتوى مبتكر يعتمد على أحدث الاتجاهات ويدعمه أفضل منهجية تعليمية وهيئة تدريس استثنائية.

إلى كل هذا، يجب أن نضيف 10 صفوف دراسية متقدمة تشكل جزءًا من المواد التعليمية، في المقدمة التكنولوجية والتعليمية. تم تصميم هذه الدروس من قبل متخصص مشهور عالميًا في الذكاء والأمن السيبراني والتقنيات التخريبية. موارد مفيدة من شأنها أن تساعد المدير التنفيذي على التخصص في إدارة الأمن السيبراني وتوجيه أقسام الشركة المخصصة لهذا المجال المهم بشكل فعال.

إنه برنامج يتم تنفيذه في 12 شهر ويتم توزيعه في 15 وحدات:

الوحدة 1	الذكاء والأمن السيبراني
الوحدة 2	الأمن في Host
الوحدة 3	أمان الشبكة (المحيط)
الوحدة 4	أمن الهواتف الذكية smartphones
الوحدة 5	الأمن في إنترنت الأشياء IoT
الوحدة 6	Hacking الأخلاقية
الوحدة 7	الهندسة العكسية
الوحدة 8	التطوير الآمن
الوحدة 9	التحليل الجنائي
الوحدة 10	التحديات الحالية والمستقبلية في أمن الحاسوب
الوحدة 11	القيادة والأخلاق والمسؤولية الاجتماعية للشركة
الوحدة 12	قيادة لأفراد وإدارة المواهب
الوحدة 13	الإدارة الاقتصادية والمالية
الوحدة 14	الإدارة التجارية والتسويق الاستراتيجي
الوحدة 15	Management الادارة

أين ومتى وكيف يتم تدريسها؟

تقدم TECH لطلابها إمكانية إجراء هذا البرنامج بالكامل عبر الإنترنت. خلال الـ 12 شهر التي يستغرقها التدريب، ستتمكن من الوصول إلى جميع محتويات هذا البرنامج في أي وقت، مما سيتيح لك إدارة وقت الدراسة بنفسك.

إنها تجربة تعليمية فريدة ومهمة وحاسمة لتعزيز تطورك المهني وتحقيق قفزة حاسمة.

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 اللاسلكى 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 Freenetg

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.الاستراتيجية الوطنية للأمن السيبراني 2019
3.8.1.مجموعة من المعايير الدولية لأمن المعلومات ISO 27032
4.8.1.إطار عمل الأمن الإلكترونى من المعهد الوطني للمعايير والتكنولوجيا
5.8.1.بك (متحكم دقيق)
6.8.1.CUGBP Elav-like family member 23072
7.8.1.اللوائح 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. INCIBE
4.10.1. منظمة الدول الأمريكية
5.10.1. أمريكا الجنوبية 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. نظام كشف التسلل القائم على المضيف
1.3.2. طرق كشف التسلل
2.3.2. Sagan
3.3.2. Aide
4.3.2. Rkhunter

4.2. Firewall المحلى
1.4.2. Firewalls Windows
2.4.2. Firewalls Linux
3.4.2. Firewalls 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 عن phishing بشكل يدوى
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. كشف نقطة النهاية والاستجابة لها 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
4.10.2. امتيازات تثبيت البرامج

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 kernel Linux
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 denyHostsg
3.4.2.3. ban2Fai

3.3. أنظمة كشف التسلل والوقاية منه (ids/ips)

1.3.3.الهجمات على ids/ips
2.3.3.أنظمة ids/ips
1.2.3.3. نظام كشف التسلل الأكثر شعبية
2.2.3.3. موتور كشف ومنع التسلل

4.3. FireWalls من الجيل التالى (ngfw)

1.4.3.الاختلافات بين ngfw و firewall التقليدى
2.4.3.القدرات الأساسية
3.4.3.حلول الأعمال
4.4.3.جدران الحماية للخدمات السحابية cloud
1.4.4.3. سحابة أمازون الافتراضية Arquitectura Cloud 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.سياقات عامة البرمجيات الخبيثة و مؤشر الالتزام
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.بوابة البريد (mgw)

8.3. إدارة المعلومات والأحداث الأمنية

1.8.3.المكونات والعمارة
2.8.3.قواعد الارتباط وحالات الاستخدام
3.8.3.التحديات الحالية لنظم إدارة المعلومات والأحداث الأمنية siem

9.3. التنسيق الأمني والأتمتة والاستجابة

1.9.3.التنسيق الأمني والأتمتة والاستجابة Soar و إدارة المعلومات والأحداث الأمنية siem: أعداء أو حلفاء
2.9.3.مستقبل أنظمة التنسيق الأمني والأتمتة والاستجابة soar

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

الوحدة 4. أمن 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. السياسات الأمنية
3.3.4. مراقبة الاجهزة
4.3.4. 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

6.4. التهديدات الرئيسية
1.6.4. مستخدم غير مجبر
2.6.4. البرمجيات الخبيثة
1.2.6.4. أنواع البرمجيات الخبيثة
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 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 على الجهاز
3.2.8.4. المثابرة
4.2.8.4. تنفيذ payload واستخراج المعلومات
3.8.4. Hacking على أجهزة iOS: الآليات والأدوات
4.8.4. Hacking على 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
SmartHome.1.2.5
SmartCity.2.2.5
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

4.5. SmartHome
1.4.5.أتمتة المنزل
2.4.5.شبكات التواصل
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.موقع
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.قابل للزرع
4.8.5.الروبوتات الجراحية

9.5. الاتصال
Wi-Fi/Gateway.1.9.5
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

الوحدة 6. Hacking أخلاقيات

1.6. بيئة العمل
1.1.6.توزيعات Linux
1.1.1.6. كالي لينكس Kali Linux - Offensive Security
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 التهرب من IDSg firewall
4.4.6.Banner Grabbing
5.4.6.مخططات الشبكة

5.6. تعداد
1.5.6.تعداد SMTP لنطاق مدرسة الأعمال
2.5.6.تعداد نظام اسم المجال
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.Session Hijacking
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 البرامج الضارة
3.3.9.6. تجاوز حلول مكافحة الفيروسات

10.6. المثابرة
1.10.6. تثبيت rootkits
2.10.6. استخدام ncat
3.10.6. استخدام المهام المجدولة للأبواب الخلفية 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. محللين 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.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 فى Linux
7.9.7.صندوق الحماية في ويندوز
8.9.7.Sandbox فى MacOS
9.9.7.Sandbox فى 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 malware

الوحدة 8. التطوير الآمن

1.8. 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 وتقويته
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
4.7.8.Hardening قاعدة 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 الجنائى

1.9. الحصول على البيانات ونسخها
1.1.9. الحصول على البيانات المتقلبة
1.1.1.9. معلومات النظام
2.1.1.9. معلومات الشبكة
3.1.1.9. ترتيب التقلب
2.1.9. الحصول على البيانات الثابتة
1.2.1.9. إنشاء صورة منسوخة
2.2.1.9. إعداد وثيقة لسلسلة الحيازة
3.1.9. طرق التحقق من صحة البيانات المكتسبة
1.3.1.9. منهجيات Linux
2.3.1.9. منهجيات Windows

2.9. تقييم تقنيات مكافحة الطب الشرعي وهزيمتها
1.2.9. أهداف تقنيات مكافحة الطب الشرعي
2.2.9. مسح البيانات
1.2.2.9. حذف البيانات والملفات
2.2.2.9. استرجاع الملفات
3.2.2.9. استرجاع الأقسام المحذوفة
3.2.9. الحماية بكلمة مرور
4.2.9. إخفاء المعلومات
5.2.9. الحذف الآمن للأجهزة
6.2.9. التشفير

3.9. التحليل الجنائي لنظام التشغيل
1.3.9. التحليل الجنائي لنظام Windows
2.3.9. التحليل الجنائي لنظام Windows
3.3.9. التحليل الجنائي لنظام Mac

4.9. التحليل الجنائي للشبكة
1.4.9. تحليل السجلات
2.4.9. ترابط البيانات
3.4.9. بحث الشبكة
4.4.9. الخطوات الواجب اتباعها في التحليل الجنائي للشبكة

5.9. التحليل الجنائي للويب
1.5.9. التحقيق في هجمات الويب
2.5.9. كشف الهجمات
3.5.9. تعقب عناوين نظام منع الاختراق IPs

6.9. التحليل الجنائي لقواعد البيانات
1.6.9. التحليل الجنائي لبرنامج قواعد البيانات العلائقية MSSQL
2.6.9. التحليل الجنائي نظام إدارة قواعد البيانات MySQL
3.6.9. التحليل الجنائي في نظام إدارة قواعد البيانات PostgreSQL
4.6.9. التحليل الجنائي في نظام قاعدة بيانات مفتوحة المصدر MongoDB

7.9. التحليل الجنائي في Cloud
1.7.9. أنواع الجرائم فى Cloud
1.1.7.9. السحابة كمشتبه
2.1.7.9. السحابة كغرض
3.1.7.9. السحابة كأداة
2.7.9. تحديات التحليل الجنائى فى Cloud
3.7.9. البحث فى خدمات التخزين Cloud
4.7.9. أدوات الادلة الجنائية Cloud

8.9. التحقيق في جرائم البريد الإلكتروني
1.8.9. أنظمة البريد
1.1.8.9. عملاء البريد
2.1.8.9. خادم البريد
3.1.8.9. خادم البريد الصادر SMTP
4.1.8.9. خادم بروتوكول مكتب البريد 3POP
5.1.8.9. خادم بروتوكول الوصول إلى رسائل الإنترنت
2.8.9. جرائم البريد
3.8.9. رسالة بريدية
1.3.8.9. رؤوس قياسية
2.3.8.9. رؤوس ممتدة
4.8.9. خطوات التحقيق في هذه الجرائم
5.8.9. 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 Subscriber Identity Module (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. شهادة
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 إلى Get Smart بدلا 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 والحوكمة
1.1.11. الحوكمة وحكومة الشركات
2.1.11. أساسيات الحوكمة المؤسسية في الشركات
3.1.11. دور مجلس الإدارة في إطار الحوكمة المؤسسية

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 التجارية 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. تنفيذ المسؤولية الاجتماعية للشركة
3.7.11. التأثير وقياس درجة المسؤولية الاجتماعية للشركات

8.11. أنظمة وأدوات الإدارة المسؤولة
1.8.11. المسؤولية الاجتماعية للشركات: المسؤولية الاجتماعية للشركات
2.8.11. القضايا الرئيسية في تنفيذ استراتيجية الإدارة المسؤولة
3.8.11. خطوات تنفيذ 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 لأفراد 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. التحليل المحتمل
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: عملية ونظام

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 الحاجات
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. الإعلامات الإدارية
1.9.12. الإعلام الداخلي والخارجي في الأعمال التجارية
2.9.12. أقسام الإعلام
3.9.12. مدير الإعلامات في الشركة ملف تعريف ديركوم

10.12. الإنتاجية وجذب المواهب واستقطابها والاحتفاظ بها وتفعيلها
1.10.12. الإنتاجية
2.10.12. عوامل جذب المواهب والاحتفاظ بها

الوحدة 13 الإدارة الاقتصادية والمالية

1.13. 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 الخزانة
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. والتخطيط 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. الصورةCash 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. التحليل الربحي

10.13.تحليل وحل الحالات/ المشاكل
1.10.13. المعلومات المالية لشركة التصميم وصناعة النسيج S.A.(INDITEX)

الوحدة 14. الإدارة التجارية والتسويق الاستراتيجي

1.14. 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. مميزات وعيوب التجارة الإلكترونية Ecommerce مقارنة بالتجارة 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 وجعل العملاء مخلصين
1.6.14. استراتيجيات الولاء والترابط 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. شركات الإعلامات
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. الإعلام 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 الادارة

1.15. 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 القيمة
3.3.15. إدارة الجودة

4.15. خطابة وتشكيل متحدثين رسميين

1.4.15. الإعلام بين الأشخاص
2.4.15. مهارات الإعلام والتأثير
3.4.15. حواجز التواصل

5.15. أدوات. الإعلامات الشخصية والتنظيمية

1.5.15. الإعلام بين الأشخاص
2.5.15. أدوات الإعلام بين الأشخاص
3.5.15. الإعلام في المنظمات
4.5.15. الأدوات في المنظمة

6.15. الإعلامات في حالات الأزمات

1.6.15. أزمات
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 والإعلام
2.8.15. الحزم والتعاطف والاستماع الفعال
3.8.15. الثقة بالنفس والإعلام العاطفي

9.15. خلق العلامات التجارية Branding الشخصية

1.9.15. استراتيجيات تطوير العلامات التجارية الشخصية
2.9.15. قوانين العلامات التجارية الشخصية
3.9.15. أدوات لبناء العلامات 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

هذا البرنامج سيفتح الأبواب أمام
عالم مهني جديد"

07

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"

تستخدم كلية إدارة الأعمال TECH 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"

يعدك هذا البرنامج لمواجهة تحديات جديدة في بيئات غير مستقرة ولتحقيق النجاح في عملك.

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

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 والعملية.

> ستتعلم، من خلال الأنشطة التعاونية والحالات الحقيقية، حل المواقف المعقدة في بيئات العمل الحقيقية "

كان منهج دراسة الحالة هو نظام التعلم الأكثر استخدامًا من قبل أفضل كليات إدارة الأعمال 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 نواجهه في منهج دراسة الحالة، وهو منهج تعلم موجه نحو الإجراءات المتخذة لحل الحالات. طوال البرنامج، 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*.

سيسمح لك نظامنا عبر الإنترنت بتنظيم وقتك ووتيرة التعلم، وتكييفه مع جداولك. يمكنك الوصول إلى المحتويات من أي جهاز ثابت أو محمول مع اتصال بالإنترنت.

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

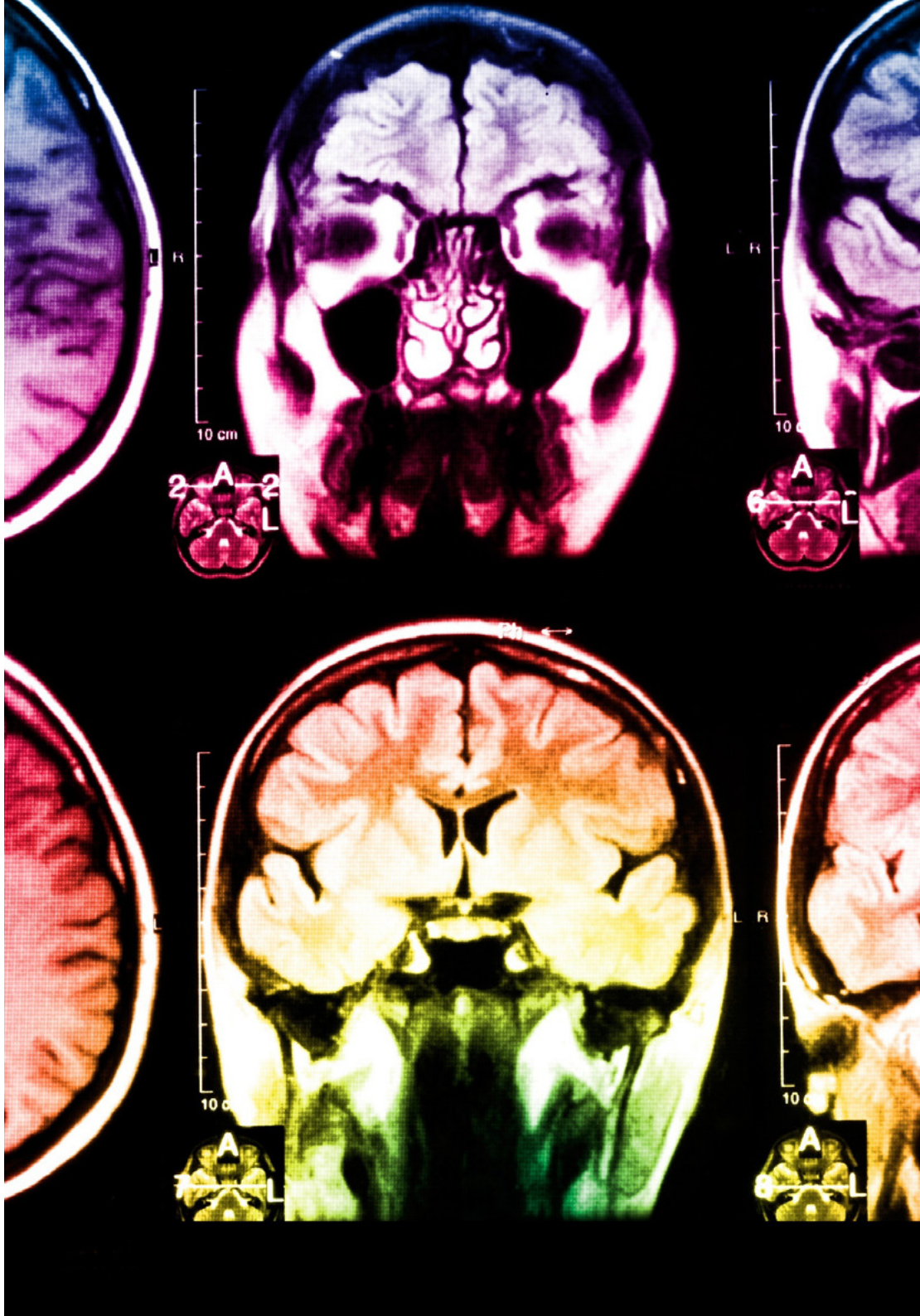
كلية إدارة الأعمال الخاصة بنا هي الكلية الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

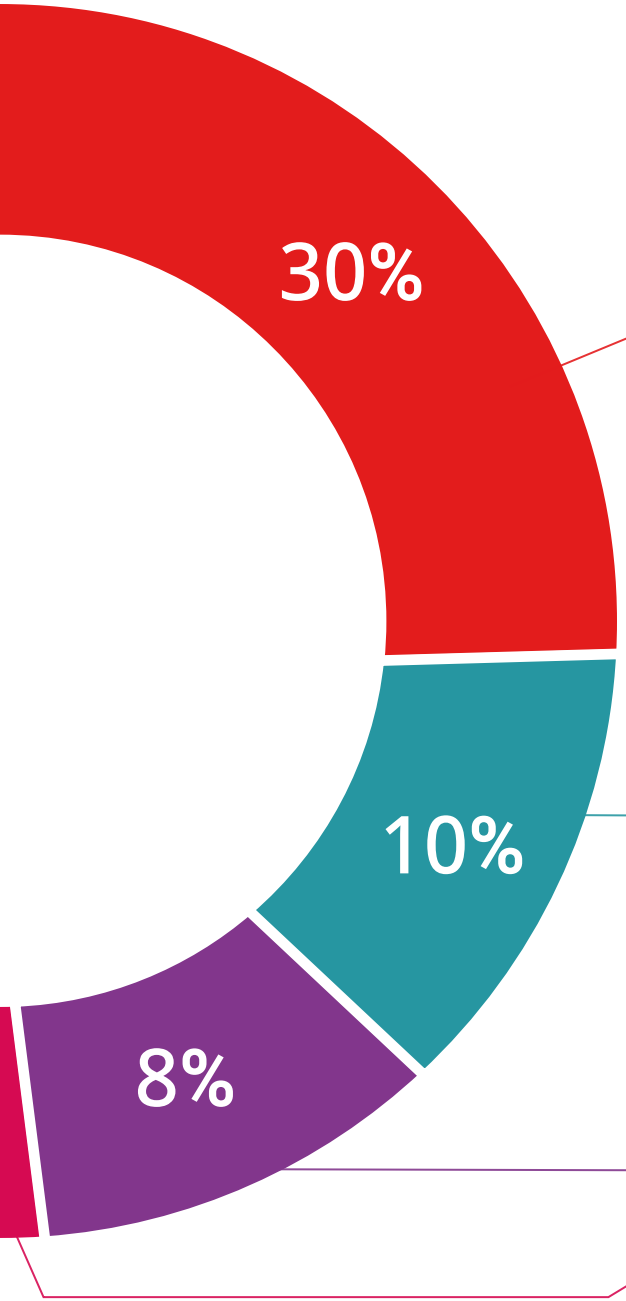
في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلّم ثم نطرح ماتعلمناه جانبًا فننساه ثم نعيد تعلمه). لذلك، نقوم بدمج كل عنصر من هذه العناصر بشكل مركزي. باستخدام هذه المنهجية، تم تدريب أكثر من 650000 خريج جامعي بنجاح غير مسبوق في مجالات متنوعة مثل الكيمياء الحيوية، وعلم الوراثة، والجراحة،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

سيضطلعون بأنشطة لتطوير كفاءات إدارية محددة في كل مجال مواضيعي. التدريب العملي والديناميكيات لاكتساب وتطوير المهارات والقدرات التي يحتاجها كبار المديرين لنموهم 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 في الإدارة العليا على الساحة الدولية.

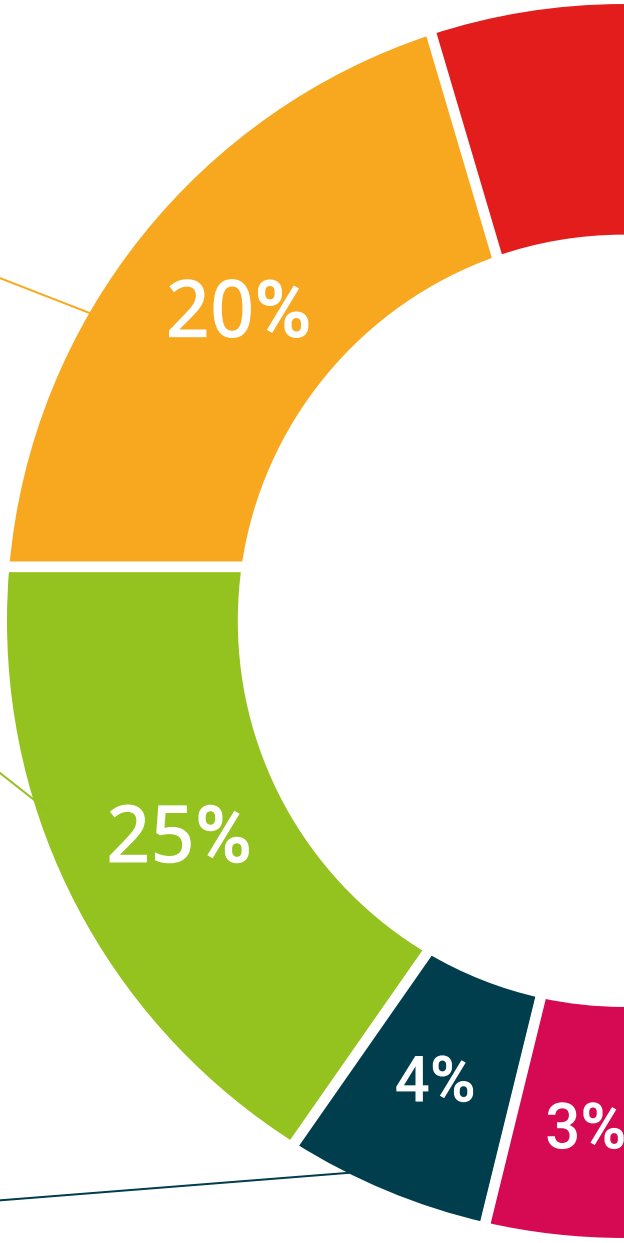
ملخصات تفاعلية

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.



08
ملف طلابنا الشخصي

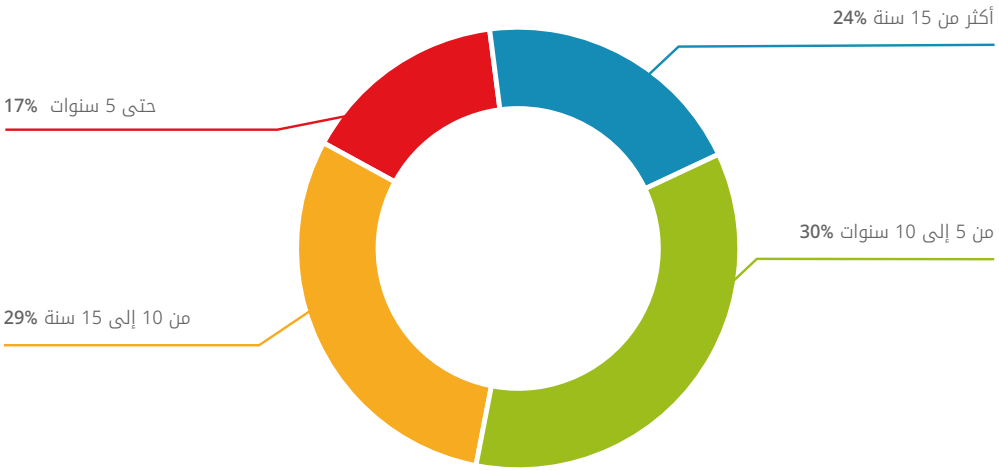
الماجستير الخاص في MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer)هو برنامج يستهدف المهنيين الذين يرغبون في تحسين تدريبهم من خلال التعليم الجيد. الطلاب الذين يرغبون في توسيع معرفتهم في فرع آخر مرتبط بالأعمال التجارية مثل علوم الحاسوب، ولكن بشكل أكثر تحديدًا مثل أمن معلومات الحاسوب. برنامج يستهدف المهنيين ذوي الخبرة، الذين يؤمنون بالتخصص العالي كوسيلة للتحسين على المستوى الشخصي والمهني.

طلاب TECH مهنيون يتمتعون بخبرة واسعة
يسعون إلى التحسين الوظيفي"

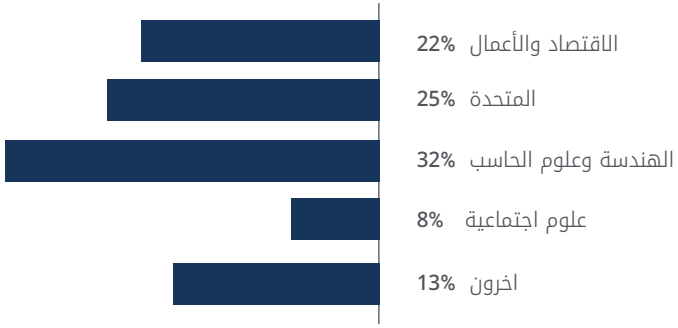
متوسط العمر

بين 35 و 45 سنة

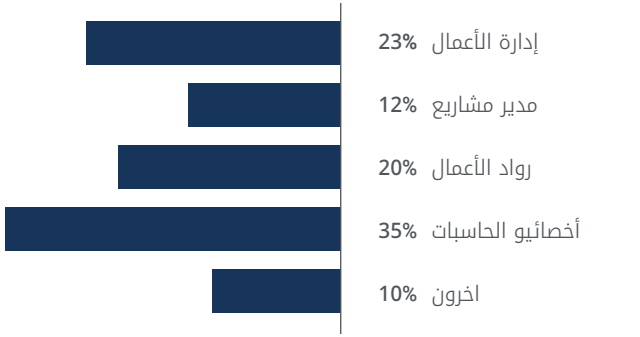
عدد سنوات الخبرة



التدريب في مجال



المؤهل الأكاديمي

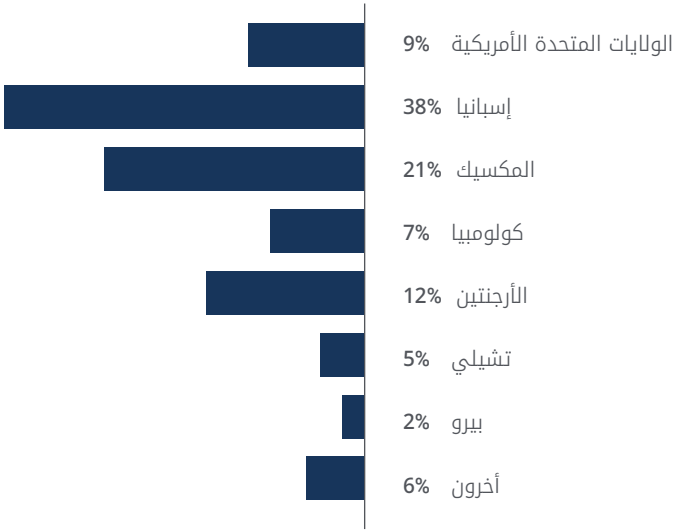


Jaime Díaz

Chief Revenue Officer

"في بيئة الأعمال التي أعمل فيها، نتعامل مع كمية كبيرة من المعلومات السرية والبيانات ذات الصلة التي يمكن أن تسبب مشكلة كبيرة للشركة في الأيدي الخطأ. لهذا السبب، كنت أفكر منذ بعض الوقت في توسيع معرفتي في مجال الأمن الإلكترونى، بهدف التحكم بنفسي في جميع العمليات التي قد تكون أكثر حساسية لتهديد الحاسوب. بفضل برنامج TECH هذا، ستتمكن من تحسين تدريبك والتصرف بمزيد من الأمان في العمل"

التوزيع الجغرافي



09

هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

مدرسو الماجستير الخاص في MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer) هم من المهنيين ذوي الخبرة الواسعة في هذا القطاع، على الصعيدين المهني والتعليمي. يتيح لهم تخصصهم في هذا المجال الحصول على المؤهلات اللازمة لتزويد الطلاب بدراسة كاملة وعالية الجودة حول موضوعات ستكون مفيدة في عملهم اليومي في مجال الأعمال. بلا شك، الأشخاص الذين يؤمنون بالتعليم العالي كوسيلة للتقدم في مهنتهم وتحسين القدرة التنافسية لأعمالهم.

طاقم تدريس يتمتع بخبرة واسعة لمساعدتك
في تخصصك في مجال الأمن الإلكترونى"

المدير الدولي المستضاف

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 حياته المهنية، قام بوضع تصور وإدارة البرامج الأكاديمية المتطورة في العديد من المؤسسات الشهيرة، مثل جامعة مونتريال، وجامعة جورج واشنطن،جامعة مونتريال، وجامعة جورج واشنطن و جامعة جورج تاون..

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 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 فيApplied Intelligence بجامعة Georgetown
- أستاذ التدريب العملى في جامعة جورج تاون
- دكتوراه في علم الجريمة من la School of Criminology جامعة Montreal
- ليسانس في علم الاجتماع وحاص على درجة Minor Degree في علم النفس من جامعة Laval
- عضو فى 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

أ. 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. فى جامعة las Islas Baleares
- مهندسة حاسوب من جامعة Alcalá de Henares في مدريد
- ماجستير في ديف أوبس: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

الأساتذة

أ. Catalá Barba, José Francisco

- فني إلكترونيات خبير في الأمن الإلكترونى
- مطور تطبيقات الهاتف المحمول
- فني إلكترونيات في القيادة المتوسطة بوزارة الدفاع الإسبانية
- فني إلكترونيات في Factoría Ford Sita في فالنسيا

أ. Jiménez Ramos, Álvaro

- محلل الأمن الإلكترونى
- كبير محللي الأمن في The Workshop
- محلل الأمن الإلكترونى L1 في Axians
- محلل الأمن الإلكترونى L2 في Axians
- محلل الأمن الإلكترونى في SACYR S.A
- شهادة في هندسة الاتصالات عن بعد من جامعة Politécnica بمدريد
- ماجستير في الأمن الإلكترونى والقرصنة الأخلاقية من المدرسة المهنية للتقنيات الجديدة CICE
- دورة عليا في الأمن الإلكترونى من قبل Deusto Formación

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
- فنية أنظمة لترحيل المعدات وإدارة وصيانة وتدريب أجهزة المساعد الرقمي الشخصي المحمولة
- مهندسة تقنية في أنظمة الكمبيوتر من جامعة Oberta في كاتالونيا
- درجة الماجستير في أمن الكمبيوتر والقرصنة الأخلاقية الرسمية من EC- Council و CompTIA من قبل المدرسة المهنية للتكنولوجيات الجديدة CICE

أ. Peralta Alonso, Jon

- مستشار أول لحماية البيانات والأمن الإلكترونى في Altia
- محامي ومستشار قانوني في Arriaga Asociados Asesoramiento Jurídico y Economía S.L
- المستشار القانوني / المتدرب في شركة مهنية: Óscar Padura
- شهادة في القانون من جامعة Pública del País Vasco
- ماجستير في حماية البيانات من مدرسة نظام المعلومات التنفيذي Innovative School
- درجة الماجستير في القانون من جامعة Pública del País Vasco
- درجة الماجستير في ممارسة الإجراءات المدنية من جامعة Internacional Isabel I de Castilla
- مدرس في درجة الماجستير في حماية البيانات الشخصية والأمن الإلكترونى وقانون تكنولوجيا المعلومات والاتصالات

أ. Redondo, Jesús Serrano

- مطور ويب وفني الأمن الإلكترونى
- 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
- مُركِّب معدات وخدمات الاتصالات في Lican Comunicaciones SL، Castilla,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

> قامت TECH باختيار فريق التدريس لهذا البرنامج بعناية حتى تتمكن من التعلم من أفضل المتخصصين اليوم.

10

مدى تأثير هذه الدراسة على حياتك المهنية

إن إكمال الماجستير الخاص فى MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer)سيضيف جودة إضافية إلى مؤهلات محترفي الأعمال، من خلال تقديم كل تلك المعرفة التي، على الرغم من أنها قد تبدو بعيدة تمامًا عن عملهم اليومي، إلا أنها يمكن أن تكون مفيدة جدًا للتحكم في أجهزة الحاسوب هذه العمليات التي قد تحتوي على بعض العناصر الخارجية الضارة التي تؤثر على المنظمة بأكملها. لذلك، يصبح التخصص العالي في هذا المجال أمرًا لا غنى عنه، سواء على المستوى الشخصي أو المهني للطلاب، ولكن أيضًا للشركات التي يطورون فيها العمالة.

تضع *TECH* جميع مواردها الأكاديمية تحت تصرف طلابها حتى يتمكنوا من اكتساب المهارات اللازمة التي تقودهم نحو النجاح"

هل أنت مستعد لأخذ قفزة للأمام فى حياتك المهنية؟
التطوير المهني الممتاز في انتظارك

الماجستير الخاص فى MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer) من TECH الجامعة التكنولوجية هو برنامج مكثف وقيم يهدف إلى تحسين مهارات عمل الطلاب في مجال الكفاءة الواسعة. بدون شك، إنها فرصة فريدة للتحسين على المستوى المهني، ولكن أيضًا على المستوى الشخصي لأنها تنطوي على الجهد والتفاني.

الطلاب الذين يرغبون في تحسين أنفسهم وتحقيق تغيير إيجابي على المستوى المهني والتفاعل مع الأفضل، سيجدون مكانهم في TECH.

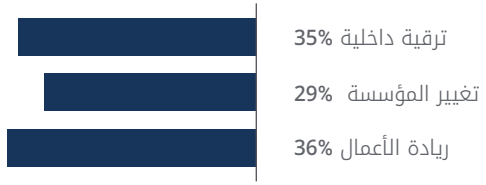
برنامج ذو مستوى أكاديمي عظيم لتوجيه حياتك المهنية نحو النجاح.

سيسمح إجراء هذا الماجستير الخاص فى MBAإ إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer) للطلاب باكتساب القدرة التنافسية اللازمة لإعطاء تحول جذري في حياتهم المهنية.

وقت التغيير

خلال دراسة البرنامج	خلال السنة الأولى	بعد سنتين
35%	30%	35%

نوع التغيير



زيادة الرواتب

دراسة هذا البرنامج يعني لطلابنا زيادة في الراتب تزيد عن **25.22%**

الراتب السابق لدراسة البرنامج	الزيادة في الراتب	الراتب اللاحق لدراسة البرنامج
€ 57.900	25.22%	€ 72.500

11

المزايا لشركتك

يساهم الماجستير الخاص فى MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer) في رفع مواهب المنظمة إلى أقصى إمكاناتها من خلال تخصص القادة رفيعي المستوى. وبهذه الطريقة، سيتمكن محترفو الأعمال من تقديم جودة إضافية لشركتهم، حيث لديهم هم أنفسهم القدرات اللازمة للتحكم في عمليات الأمن الإلكترونية. برنامج يتكيف مع الطلاب حتى يكتسبوا الأدوات اللازمة التي يمكنهم تطبيقها لاحقًا في ممارستهم اليومية، مما يحقق فوائد كبيرة لشركتهم.

برنامج لا غنى عنه لمحترفي الأعمال الذين يرغبون في التحكم في مشكلات الأمن الإلكترونية المحتملة وإدارتها.

يعد تطوير المواهب والاحتفاظ بها في الشركات أفضل استثمار طويل الأجل.

01

رأس المال الفكري ونمو المواهب

سيقدم المسؤول التنفيذي الشركة إلى المفاهيم والاستراتيجيات ووجهات النظر الجديدة التي يمكن أن تحدث تغييرات كبيرة في المنظمة.

02

الاحتفاظ بالمديرين التنفيذيين ذوي الإمكانات العالية لتجنب استنزاف المواهب

يعزز هذا البرنامج الصلة بين الشركة والمدير ويفتح آفاقًا جديدة للنمو المهني داخل الشركة.

03

وكلاء البناء للتغيير

ستكون قادرًا على اتخاذ القرارات في أوقات عدم اليقين، والأزمات مما يساعد المنظمة في التغلب على العقبات.

04

زيادة إمكانيات التوسع الدولي

بفضل هذا البرنامج، ستتواصل الشركة مع الأسواق الرئيسية في الاقتصاد العالمي.

05 تطوير مشاريع شخصية

يمكن للمهني العمل في مشروع حقيقي أو تطوير مشاريع جديدة في نطاق البحث والتطوير أو تطوير الأعمال في شركتك.

06 تعزيز القدرة التنافسية

سيزود هذا البرنامج مهنييه بالمهارات لمواجهة التحديات الجديدة وبالتالي تعزيز المؤسسة.

12

المؤهل العلمى

يضمن ماجستير الخاص فى MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer) التدريب الأكثر دقة وحداثة بالإضافة إلى الحصول على مؤهل الماجستير الخاص الصادرة عن TECH الجامعة التكنولوجية.

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

هذه **ماجستير خاص في MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer)** 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 الإلكترونى (CISO, Chief Information Security Officer)**

اطريقة: **عبر الإنترنت**

مدة: **12 أشهر**


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 الإلكترونى
(CISO, Chief Information Security Officer)

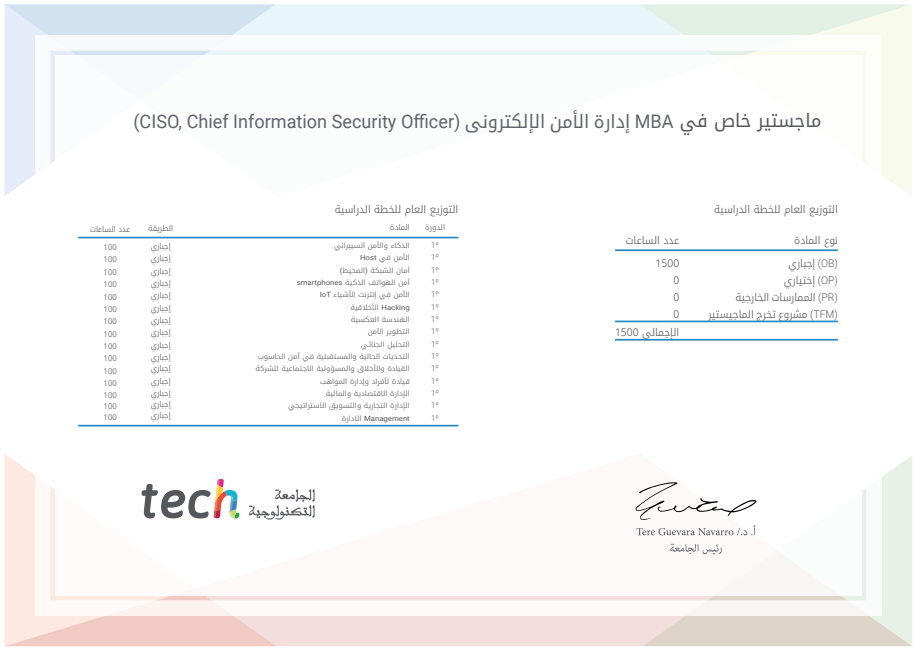
وهي شهادة خاصة من هذه الجامعة موافقة لـ 1500
ساعة، مع تاريخ بدء يوم/شهر/ سنة وتاريخ انتهاء يوم/شهر/سنة

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

في تاريخ 17 يونيو 2020

Tere Guevara Navarro أ. د./
رئيس الجامعة

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


ماجستير خاص في MBA إدارة الأمن الإلكترونى (CISO, Chief Information Security Officer)

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 السيبرانى	إجبارى	100
1°	الأمن فى Host	إجبارى	100
1°	أمان الشبكة (المحيط)	إجبارى	100
1°	أمن الهواتف الذكية smartphones	إجبارى	100
1°	الأمن فى إنترنت الأشياء IoT	إجبارى	100
1°	Hacking الأخلاقية	إجبارى	100
1°	الهندسة العكسية	إجبارى	100
1°	التطوير الأمن	إجبارى	100
1°	التحليل الجنائى	إجبارى	100
1°	التحديات الحالية والمستقبلية فى أمن الحاسوب	إجبارى	100
1°	القيادة والأخلاق والمسؤولية الاجتماعية للشركة	إجبارى	100
1°	قيادة الأفراد وإدارة المواهب	إجبارى	100
1°	الإدارة الاقتصادية والمالية	إجبارى	100
1°	الإدارة التجارية والتسويق الاستراتيجى	إجبارى	100
1°	Management الادارة	إجبارى	100

tech الجامعة التكنولوجية

Tere Guevara Navarro أ. د./
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

ماجيستير خاص
MBA إدارة الأمن الإلكترونى
(CISO, Chief Information Security Officer)

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

ماجيستير خاص
MBA إدارة الأمن الإلكترونى
(CISO, Chief Information Security Officer)

tech الجامعة التيكنولوجية