ماجيستير خاص
MBA إدارة الأمن السيبراني المتقدم (CISO)

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

ماجيستير خاص
MBA إدارة الأمن السيبراني المتقدم (CISO)

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

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

الفهرس

01

المقدمة

يتجه العالم اليوم نحو الرقمنة الكاملة. يتم تنفيذ المزيد والمزيد من العمليات الأساسية والعمليات والمهام بجميع أنواعها من خلال جهاز إلكتروني. لكن هذا التقدم يأتي أيضاً مع بعض المخاطر، حيث يمكن أن تكون أجهزة الكمبيوتر والهواتف الذكية والأجهزة اللوحية وجميع أنواع التطبيقات الرقمية عرضة للهجمات الإلكترونية. لهذا السبب، تبحث العديد من الشركات عن خبراء قادرين على قيادة وإدارة الأمن السيبراني لخدماتها بفعالية. هناك طلب كبير على هذا الملف المهني الجديد، لذا فقد تم تصميم هذا البرنامج لتوفير أحدث المعارف والتقنيات لعالم الحاسوب الذي سيكون مستعداً ليكون مديراً للأمن السيبراني في أي شركة تتطلب ذلك.

سيعدك هذا البرنامج إعداداً مكثفاً للتخصص في إدارة الأمن السيبراني، وهو الملف المهني الأكثر طلباً في مجال تكنولوجيا المعلومات اليوم"

تسارعت عملية الرقمنة في السنوات الأخيرة، مدفوعة بالتقدم المستمر في تكنولوجيا المعلومات. بالتالي، لم يقتصر الأمر على التكنولوجيا التي تمتعت بتحسينات كبيرة فحسب، بل أيضًا الأدوات الرقمية ذاتها التي يتم بها تنفيذ العديد من المهام اليوم. على سبيل المثال، أتاحت هذه التطورات إمكانية إجراء العديد من المعاملات المصرفية من تطبيق الهاتف المحمول. كما حدثت تطورات جديدة في قطاع الرعاية الصحية، في أنظمة وأنظمة المواعيد والوصول إلى السجلات الطبية. بالإضافة إلى ذلك، بفضل هذه التقنيات، من الممكن الاطلاع على الفواتير أو طلب الخدمات من الشركات في مجالات مثل الاتصالات الهاتفي

لكن هذه التطورات أدت أيضاً إلى زيادة نقاط الضعف في الحواسيب. بالتالي، بينما توسعت خيارات أداء الأنشطة والمهام المختلفة، ازدادت الهجمات على أمن الأجهزة والتطبيقات والمواقع الإلكترونية بشكل متناسب. نتيجة لذلك، يتزايد عدد الشركات التي تبحث عن متخصصين في مجال الأمن السيبراني قادرين على توفير الحماية الكافية لها ضد جميع أنواع الهجمات الإلكترونية.

بالتالي، فإن وظيفة مدير الأمن السيبراني هي واحدة من أكثر الوظائف المطلوبة من قبل الشركات التي تعمل على الإنترنت أو لديها خدمات في البيئة الرقمية. للاستجابة لهذا الطلب، صممت TECH ماجستير MBA في إدارة الأمن السيبراني المتقدم (CISO)، والذي سيزود عالم الحاسوب بجميع الأدوات اللازمة للقيام بهذا المنصب بفعالية ووفقًا لأحدث التطورات في الحماية ونقاط الضعف في هذا المجال التكنولوجي.

ستتمكن في هذا البرنامج من دراسة جوانب متعمقة مثل الأمن في تطوير وتصميم الأنظمة، وأفضل تقنيات التشفير والأمن في بيئات الحوسبة السحابية. ستقوم بذلك من خلال منهجية متاحة 100% عبر الإنترنت، حيث ستتمكن من الجمع بين عملك المهني ودراستك، دون جداول زمنية صارمة أو رحلات غير مريحة إلى مركز أكاديمي. ستستفيد أيضًا من العديد من الموارد التعليمية متعددة الوسائط، والتي يقوم بتدريسها أعضاء هيئة التدريس الأكثر شهرة وتخصصًا في مجال الأمن السيبراني.

يحتوي هذا **الماجستير الخاص في MBA في إدارة الأمن السيبراني المتقدم (CISO)** على البرنامج التعليمي الأكثر اكتمالاً وحداثة في السوق. أبرز خصائصها هي:

- تطوير الحالات العملية التي يقدمها الخبراء في تكنولوجيا المعلومات الذكاء السيبراني
- محتوياتها البيانية والتخطيطية والعملية البارزة التي يتم تصورها بها تجمع المعلومات العلمية والرعاية العملي حول تلك التخصصات الأساسية للممارسة المهنية
- التمارين العملية حيث يمكن إجراء عملية التقييم الذاتي لتحسين التعلم
- تركيزها على المنهجيات المبتكرة
- دروس نظرية، أسئلة للخبير، منتديات نقاش حول مواضيع مثيرة للجدل وأعمال التفكير الفردي
- توفر المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

> تعلم بشكل مباشر أفضل تقنيات الأمن المطبقة على بيئات Cloud Computing أو تقنية Blockchain"

سوف تستمتع بالعديد من محتويات
الوسائط المتعددة لتسريع عملية التعلم
الخاصة بك، بينما تتلقى الدعم من المعلمين
المرموقين في مجال الأمن السيبراني"

ستسمح لك منهجية TECH عبر الإنترنت باختيار
الوقت والمكان للدراسة، دون إعاقة عملك المهني.

ستتمكن من أن تصبح مدير الأمن
السيبراني لأفضل الشركات في منطقتك.

البرنامج يضم، في أعضاء هيئة تدريسه محترفين في المجال المتجددة يصبون في هذا التدريب خبرة عملهم، بالإضافة إلى متخصصين معترف بهم من الشركات 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 الدراسي. للقيام بذلك، سيحصل على مساعدة من نظام فيديو تفاعلي مبتكر من قبل خبراء مشهورين.

02

الأهداف

أدى التطور السريع لتكنولوجيا المعلومات إلى تحقيق تقدم كبير في مجال تكنولوجيا المعلومات، مما أدى إلى توفير العديد من الخدمات للسكان بشكل عام. مع ذلك، فقد ازداد عدد الثغرات والهجمات السيبرانية أيضاً، لذا فإن الهدف الرئيسي من هذا البرنامج هو تحويل عالم الحاسوب إلى متخصص حقيقي في إدارة الأمن السيبراني، مما يضمن له تقدماً مهنياً هائلاً وفورياً. ستوفر لك مهاراتك الجديدة فرصة الوصول إلى شركات كبيرة نشطة رقمياً في مختلف القطاعات.

الهدف من هذا البرنامج هو جعلك محترفاً مستعداً
لقيادة قسم الأمن السيبراني في شركة كبيرة"

الأهداف العامة

- توليد المعرفة المتخصصة حول نظام المعلومات وأنواعه والجوانب الأمنية التي يجب أخذها في ال
- تحديد نقاط الضعف في نظام المعلومات
- تطوير التنظيم القانوني وتجريم الاعتداء على نظام المعلوماتية
- تقييم نماذج البنية الأمنية المختلفة لتحديد النموذج الأنسب للمؤسسة
- تحديد الأطر التنظيمية المعمول بها والأسس التنظيمية لها
- تحليل الهيكل التنظيمي والوظيفي لمجال أمن المعلومات (مكتب CISO)
- تحليل وتطوير مفهوم المخاطرة وعدم اليقين في البيئة التي نعيش فيها
- فحص نموذج إدارة المخاطر استنادًا إلى ISO 31.000
- دراسة علم التشفير وعلاقته بفروعه: علم التشفير وتحليل الشفرات وعلم إخفاء المعلومات وتحليل إخفاء المعلومات
- تحليل أنواع التشفير وفقاً لنوع الخوارزمية ووفقاً لاستخدامها
- فحص الشهادات الرقمية
- فحص البنية التحتية للمفاتيح العامة (PKI)
- تطوير مفهوم إدارة الهوية
- تحديد طرق المصادقة
- توليد المعرفة المتخصصة حول منظومة أمن الحاسبات
- تقييم المعرفة بالأمن السيبراني
- تحديد مجالات الأمن فيCloud
- تحليل الخدمات والأدوات في كل مجال من مجالات الأمن
- تطوير مواصفات الأمن لكل تقنية من تقنيات شبكات LPWAN الطاقة المنخفضة
- تحليل مقارن لأمن تقنيات شبكات LPWAN منخفضة الترددات

الأهداف المحددة

الوحدة 1. السلامة في التصميم وتطوير الأنظمة

- تقييم أمن نظام المعلومات بجميع مكوناته وطبقاته.
- التعرف على أنواع التهديدات الأمنية الحالية واتجاهاتها
- وضع المبادئ التوجيهية الأمنية من خلال تحديد سياسات وخطط الأمن والطوارئ
- تحليل الاستراتيجيات والأدوات اللازمة لضمان سلامة وأمن نظم المعلومات
- تطبيق التقنيات والأدوات المحددة لكل نوع من أنواع الهجمات أو الثغرات الأمنية
- حماية المعلومات الحساسة المخزنة في نظام المعلومات
- أن يكون لدينا الإطار القانوني وتصنيف الجريمة، واستكمال الرؤية بتصنيف الجاني والمجني عليه

الوحدة 2. هياكل ونماذج أمن المعلومات

- مواءمة الخطة الرئيسية الأمنية مع الأهداف الاستراتيجية للمؤسسة
- إنشاء إطار عمل مستمر لإدارة المخاطر كجزء لا يتجزأ من الخطة الرئيسية الأمنية
- تحديد المؤشرات الملائمة لرصد تنفيذ نظام إدارة نظم إدارة المعلومات الإدارية المتكاملة
- وضع استراتيجية أمنية قائمة على السياسات
- تحليل الأهداف والإجراءات المرتبطة بخطة توعية الموظفين والموردين والشركاء
- تحديد اللوائح والشهادات والقوانين المنطبقة على كل مؤسسة ضمن الإطار التنظيمي
- تطوير العناصر الأساسية التي يتطلبها معيار ISO 27001:2013
- تنفيذ نموذج إدارة الخصوصية بما يتماشى مع اللوائح الأوروبية اللائحة العامة لحماية البيانات/اللائحة العامة لحماية البيانات

الوحدة 3. إدارة الأمن IT

- التعرف على الهياكل المختلفة التي يمكن أن تحتويها منطقة أمن المعلومات
- تطوير نموذج أمني يستند إلى ثلاثة خطوط دفاعية
- عرض اللجان الدورية والاستثنائية المختلفة التي يشارك فيها مجال الأمن السيبراني
- تحديد الأدوات التكنولوجية التي تدعم الوظائف الرئيسية لفريق العمليات الأمنية (SOC)
- تقييم تدابير التحكم في نقاط الضعف المناسبة لكل سيناريو
- تطوير إطار العمليات الأمنية استنادًا إلى إطار عمل المعهد الوطني للمعايير والمقاييس والمواصفات الأمنية
- تحديد نطاق الأنواع المختلفة من عمليات التدقيق (Red Team، Pentesting، Bug Bounty، etc)
- اقتراح الأنشطة التي سيتم تنفيذها بعد وقوع حادث أمني
- إنشاء مركز قيادة لأمن المعلومات يشمل جميع الجهات الفاعلة ذات الصلة (السلطات والعملاء والموردين وما إلى ذلك)

الوحدة 4. تحليل المخاطر وبيئة أمن تكنولوجيا المعلومات

- دراسة البيئة التي نتحرك فيها بنظرة شمولية
- تحديد المخاطر والفرص الرئيسية التي قد تؤثر على تحقيق أهدافنا
- تحليل المخاطر على أساس أفضل الممارسات المتاحة لنا
- تقييم الأثر المحتمل لهذه المخاطر والفرص
- تطوير التقنيات التي تسمح لنا بالتعامل مع المخاطر والفرص بطريقة تزيد من قيمة المساهمة
- دراسة متعمقة للتقنيات المختلفة لتحويل المخاطر والقيمة
- توليد قيمة من تصميم النماذج الخاصة لإدارة المخاطر الرشيقة
- فحص النتائج لاقتراح تحسينات مستمرة في إدارة المشاريع والعمليات استنادًا إلى نماذج الإدارة القائمة على المخاطر.Risk-Driven
- ابتكار البيانات العامة وتحويلها إلى معلومات ذات صلة لاتخاذ القرارات القائمة على المخاطر

الوحدة 5. التشفير في تكنولوجيا المعلومات

- تجميع العمليات الأساسية (XOR، الأعداد الكبيرة، الاستبدال والتحويل) والمكونات المختلفة (الوظائف أحادية الاتجاه، التجزئة، مولدات الأرقام العشوائية)
- تحليل تقنيات التشفير
- تطوير خوارزميات التشفير المختلفة
- توضيح استخدام التوقيعات الرقمية وتطبيقها في الشهادات الرقمية
- تقييم أنظمة إدارة المفاتيح وأهمية أطوال مفاتيح التشفير
- دراسة خوارزميات اشتقاق المفاتيح
- تحليل دورة حياة المفاتيح
- تقييم أوضاع تشفير الكتل وتشفير التدفق
- تحديد مولدات الأرقام العشوائية الزائفة
- تطوير حالات تطبيق التشفير في العالم الحقيقي، مثل Kerberos أو PGP
- فحص الجمعيات والهيئات ذات الصلة، مثل ISO أو NIST أو NCSC
- تحديد التحديات في التشفير في الحوسبة الكمية

الوحدة 6. إدارة الهوية والوصول في أمن تكنولوجيا المعلومات

- تطوير مفهوم الهوية الرقمية
- تقييم التحكم المادي في الوصول إلى المعلومات
- الأساس المنطقي للمصادقة البيومترية ومصادقة MFA
- تقييم الاعتداءات المتعلقة بسرية المعلومات
- تحليل اتحاد الهويات
- إنشاء التحكم في الوصول إلى الشبكة

الوحدة 7. الأمن في الاتصالات وتشغيل البرامج

- تطوير الخبرة في مجال الأمن المادي والمنطقي
- إظهار المعرفة بالاتصالات والشبكات
- تحديد الهجمات الخبيثة الرئيسية
- إنشاء إطار تطوير آمن
- إثبات فهم اللوائح التنظيمية الرئيسية لنظام إدارة أمن المعلومات
- تأسيس تشغيل مركز عمليات الأمن السيبراني
- توضيح أهمية وجود ممارسات الأمن السيبراني في مواجهة الكوارث المؤسسية للكوارث التنظيمية

الوحدة 8. الأمن في البيئات السحابية

- تحديد مخاطر نشر البنية الأساسية السحابية العامة Cloud
- تحديد المتطلبات الأمنية
- وضع خطة أمنية للنشر السحابيCloud
- تحديد الخدمات السحابية Cloudالتي سيتم نشرها لتنفيذ خطة الأمن
- تحديد الترتيبات التشغيلية اللازمة للآليات الوقائية
- وضع مبادئ توجيهية لنظام Loggingالتسجيل والمراقبة
- اقتراح إجراءات الاستجابة للحوادث

الوحدة 9. أمن اتصالات أجهزة إنترنت الأشياء

- تقديم بنية إنترنت الأشياء المبسطة
- تبرير الفروق بين تقنيات الاتصال العامة وتقنيات الاتصال الخاصة بإنترنت الأشياء
- ترسيخ مفهوم المثلث الحديدي لاتصال إنترنت الأشياء
- تحليل المواصفات الأمنية لتقنية LoRaWAN
  تقنية NB-IoT وتقنية WiSUN
- تبرير اختيار تقنية إنترنت الأشياء المناسبة لكل مشروع

الوحدة 10. خطة استمرارية الأعمال المرتبطة بالأمن

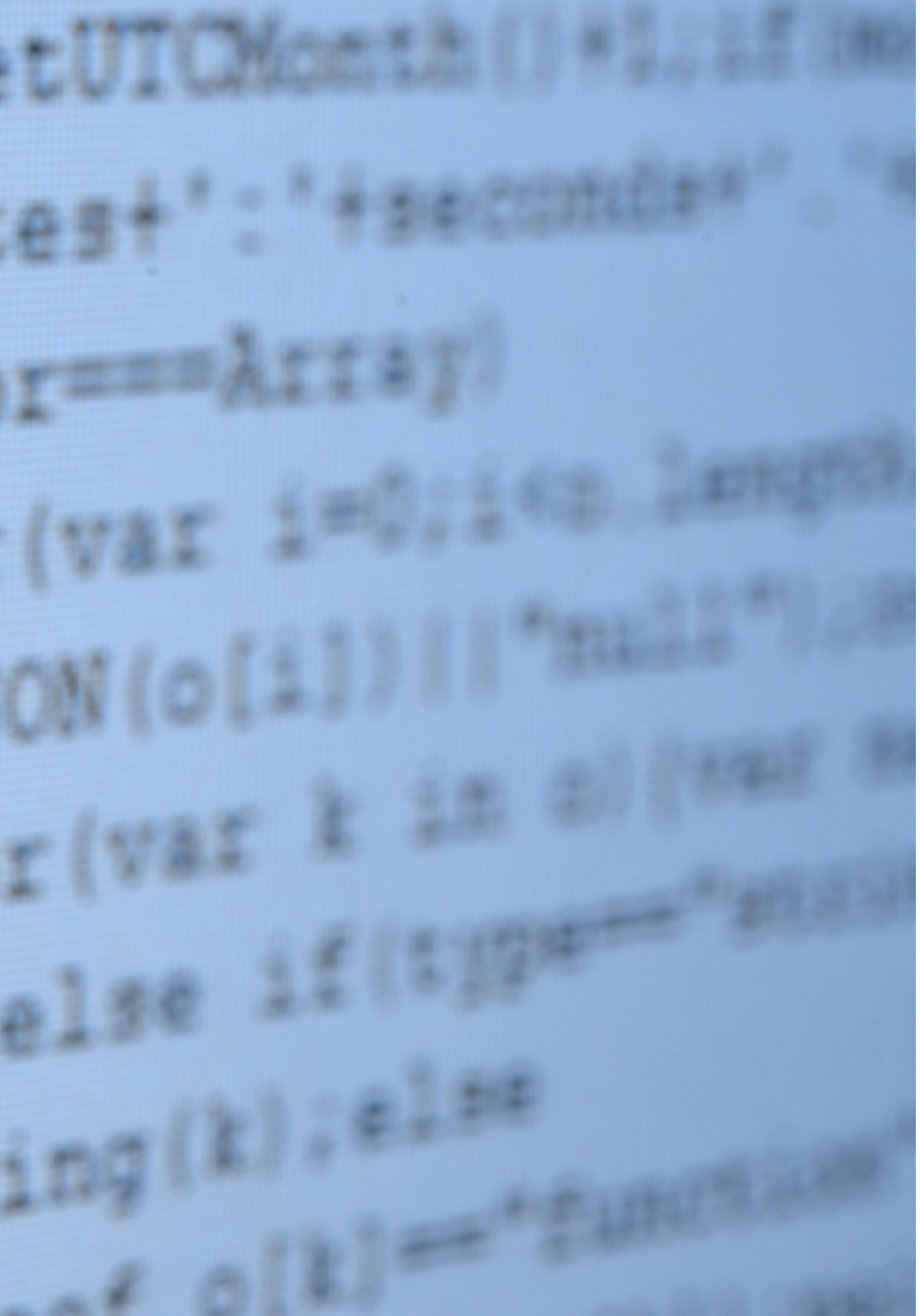
- عرض العناصر الرئيسية لكل مرحلة وتحليل خصائص خطة استمرارية الأعمال (BCP)
- إثبات الحاجة إلى خطة استمرارية الأعمال
- تحديد خرائط النجاح والمخاطر لكل مرحلة من مراحل خطة استمرارية الأعمال
- تحديد كيفية وضع خطة عمل للتنفيذ
- تقييم مدى اكتمال خطة استمرارية الأعمال (PCN)
- وضع خطة للتنفيذ الناجح لخطة استمرارية الأعمال

الوحدة 11. القيادة والأخلاق والمسؤولية الاجتماعية للشركة

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

الوحدة 12. قيادة لأفراد وإدارة المواهب

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



الوحدة 13. الإدارة الاقتصادية والمالية

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

الوحدة 14. الإدارة التجارية والتسويق الاستراتيجي

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

الوحدة 15. الإدارة التنفيذية (Management)

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

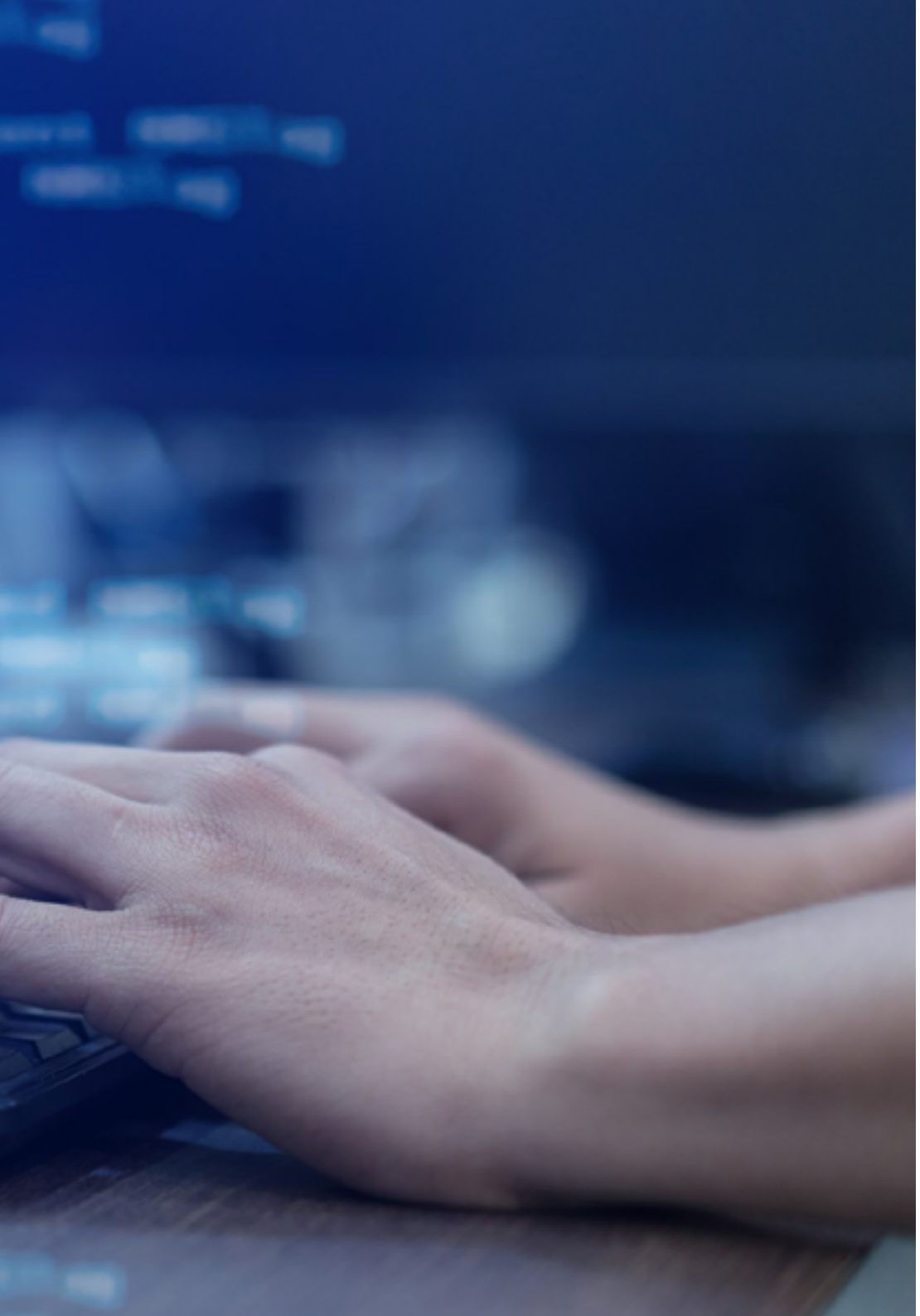
ستصبح أهدافك المهنية الآن في متناول يدك بفضل درجة الماجستير الخاص هذه، التي تتمتع بالمعرفة الأكثر تقدمًا في مجال الأمن السيبراني"

03

الكفاءات

بفضل درجة الماجستير الخاص هذه، سيكتسب المحترف العديد من الكفاءات الجديدة في مجال الأمن السيبراني. أدى ظهور تقنيات مثل البلوك تشين والحوسبة السحابيةCloud Computing والذكاء الاصطناعي في السنوات الأخيرة إلى تطوير مجالات جديدة للأمن السيبرانيا. لهذا السبب، تم تصميم هذا البرنامج خصيصاً لتزويد المحترفين بجميع المهارات اللازمة للتكيف مع هذه التقنيات المزدهرة.

المهارات التي سيوفرها لك هذا البرنامج ستسمح لك بالتحديث والتكيف مع بيئة الحوسبة الجديدة، حيث ظهرت تقنيات مثل Blockchain أو الذكاء الاصطناعي بقوة"



الكفاءات العامة

- تطبيق التدابير الأمنية الأكثر ملاءمة حسب التهديدات
- تحديد سياسة وخطة أمن نظم المعلومات الخاصة بالشركة، واستكمال تصميم وتنفيذ خطة الطوارئ
- إنشاء برنامج تدقيق يلبي احتياجات التقييم الذاتي للأمن السيبراني للمؤسسة
- تطوير برنامج لمسح ومراقبة الثغرات الأمنية وخطة استجابة لحوادث الأمن السيبراني
- تعظيم الفرص المتاحة والتخلص من التعرض لجميع المخاطر المحتملة من التصميم نفسه
- تجميع أنظمة الإدارة الرئيسية
- تقييم أمن المعلومات في الشركة
- تحليل أنظمة الوصول إلى المعلومات
- تطوير أفضل الممارسات في التطوير الآمن
- عرض المخاطر التي تتعرض لها الشركات من عدم وجود بيئة آمنة لتكنولوجيا المعلومات

الكفاءات المحددة

- تطوير نظام إدارة أمن المعلومات (SGSI)
- تحديد العناصر الرئيسية التي يتكون منها نظام إدارة نظم إدارة أمن المعلومات
- تطبيق منهجية MAGERIT لتطوير النموذج والمضي به خطوة إلى الأمام
- تصميم منهجيات جديدة لإدارة المخاطر، بناءً على مفهوم agile Risk Management
- تحديد وتحليل وتقييم ومعالجة المخاطر التي يواجهها المحترف من منظور تجاري جديد يعتمد على نموذج Risk-Driven أو مدفوع بالمخاطر والذي لا يسمح فقط بالبقاء في بيئته الخاصة، ولكن أيضًا لتعزيز مساهمة القيمة الخاصة بالفرد
- فحص عملية تصميم استراتيجية الأمن عند نشر خدمات السحابة Cloud للشركات
- تقييم الاختلافات في التطبيقات الملموسة لموردي Cloud العامة المختلفين
- تقييم خيارات الاتصال بإنترنت الأشياء للتعامل مع المشروع، مع التركيز بشكل خاص على تقنيات LPWAN
- تقديم المواصفات الأساسية لتقنيات شبكات LPWAN الرئيسية لإنترنت الأشياء

04

هيكل الإدارة وأعضاء هيئة تدريس الدورة التدريبية

يتطلب التعقيد الهائل للأمن السيبراني اليوم عملية تعلم شاملة ومفصلة. لهذا السبب، أخذ جامعة TECH على عاتقه جمع أفضل أعضاء هيئة التدريس المتخصصين في هذا المجال. بالتالي، سيتمتع المحترف بدعم وإشراف فريق تدريس مطلع على أحدث التطورات في هذا المجال، حتى يتمكنوا من دمج أفضل تقنيات الأمن السيبراني في عملهم اليومي، مع اكتساب المهارات الإدارية اللازمة في هذا المجال. منطقة.

سيكون لديك متخصصون حقيقيون في الأمن السيبراني تحت تصرفك. هذه هي الفرصة التي كنت أبحث عنها"

المدير الدولي المستضاف

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 عليا في العديد من المؤسسات التكنولوجية في العديد من الشركات المدرجة على قائمة Fortune 50، بما في ذلك NBCUniversal و Comcast.
وقد مكّنها سجلها 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 اجازة في التواصل التنظيمي من جامعة Miami، 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، استقطاب المواهب، 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 Miami

تضم جامعة TECH مجموعة متميزة ومتخصصة من المديرين الدوليين المستضافيين الذين يشغلون مناصب قيادية مهمة في أكثر الشركات تطوراً في السوق العالمية"

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 هندسة 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 الشأن 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، والقياس و الإسناد. 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، Siemens، 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 Eaton، 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 أرماني للصرافة في جورجيو أرماني، 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 Machine Learningg IA في UC Berkeley Colleg of Engineering
- MBA التنفيذي في التجارة الإلكترونية في جامعة Copenhague
- اجازة وماجستير في الرياضيات والإحصاء في جامعة Copenhague

"ادرس في أفضل جامعة أونلاين في العالم حسب مجلة 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 عامًا 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. ترفيه (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 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 Florida، Estados Unidos. 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.

ترك Nyquist 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 الإعلامات 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
- 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 هذا المؤهل الجامعي 100%، ستتمكن من الجمع بين دراستك والتزاماتك اليومية، بمساعدة كبار الخبراء الدوليين في مجال اهتمامك. سجل الآن!

هيكل الإدارة

أ. Olalla Bonal, Martín

- كبير مديري ممارسات Blockchain في EY
- أخصائي فني عميل Blockchain لشركة IBM
- مدير الهندسة المعمارية ل Blocknitive
- منسق من فريق في قواعد البيانات الموزعة غير العلائقية لشركة wedoIT (شركة IBM الفرعية)
- مهندس البنية التحتية في Bankia
- رئيس قسم التخطيط في T-Systems
- منسق القسم لشركة Bing Data España.شركة ذات مسؤولية SL

الأساتذة

د. Nogales Ávila, Javier

- استشاري أول في مجال الحوسبة السحابية المؤسسية والتوريد Quint
- مستشار الحوسبة السحابية والتكنولوجيا. Indra
- استشاري تقني مشارك. Accenture
- متخرج من جامعة Jaén وجامعة Technology and Economics في بودابست (BME)
- إجازة في الهندسة لكلية التنظيم الصناعية

أ. Mérida Téllez, Juan Manuel

- شريك مؤسس في شركة Ismet Tech
- مدير أمن المعلومات في مجموعة Ecix Group
- Operational Security Officer في شركة Atos لحلول وخدمات تكنولوجيا المعلومات A/S
- محاضر في إدارة الأمن السيبراني في الدراسات الجامعية
- بكالوريوس في علم الهندسة من جامعة Valladolid
- ماجستير في نظم الإدارة المتكاملة من جامعة CEU San Pablo

الأساتذة

أ. Gonzalo Alonso, Félix

- العضو المنتدب والمؤسس في Smart REM Solutions
- شريك مؤسس ورئيس قسم هندسة المخاطر والابتكار. Dynargy
- العضو المنتدب والشريك المؤسس Risknova (مكتب الخبراء المتخصص في التكنولوجيا)
- بكالوريوس الهندسة في التقنيات الصناعية من الجامعةICAE Pontificia Comillas(المعهد الكاثوليكي للفنون والصناعات)
- خريج الهندسة في التقنيات الصناعية من الجامعةICAE Pontificia Comillas(المعهد الكاثوليكي للفنون والصناعات)
- درجة الماجستير في إدارة التأمين من معهد التعاون بين شركات التأمين ICEA (معهد التعاون بين شركات التأمين)

د. Pascual، Alejandro

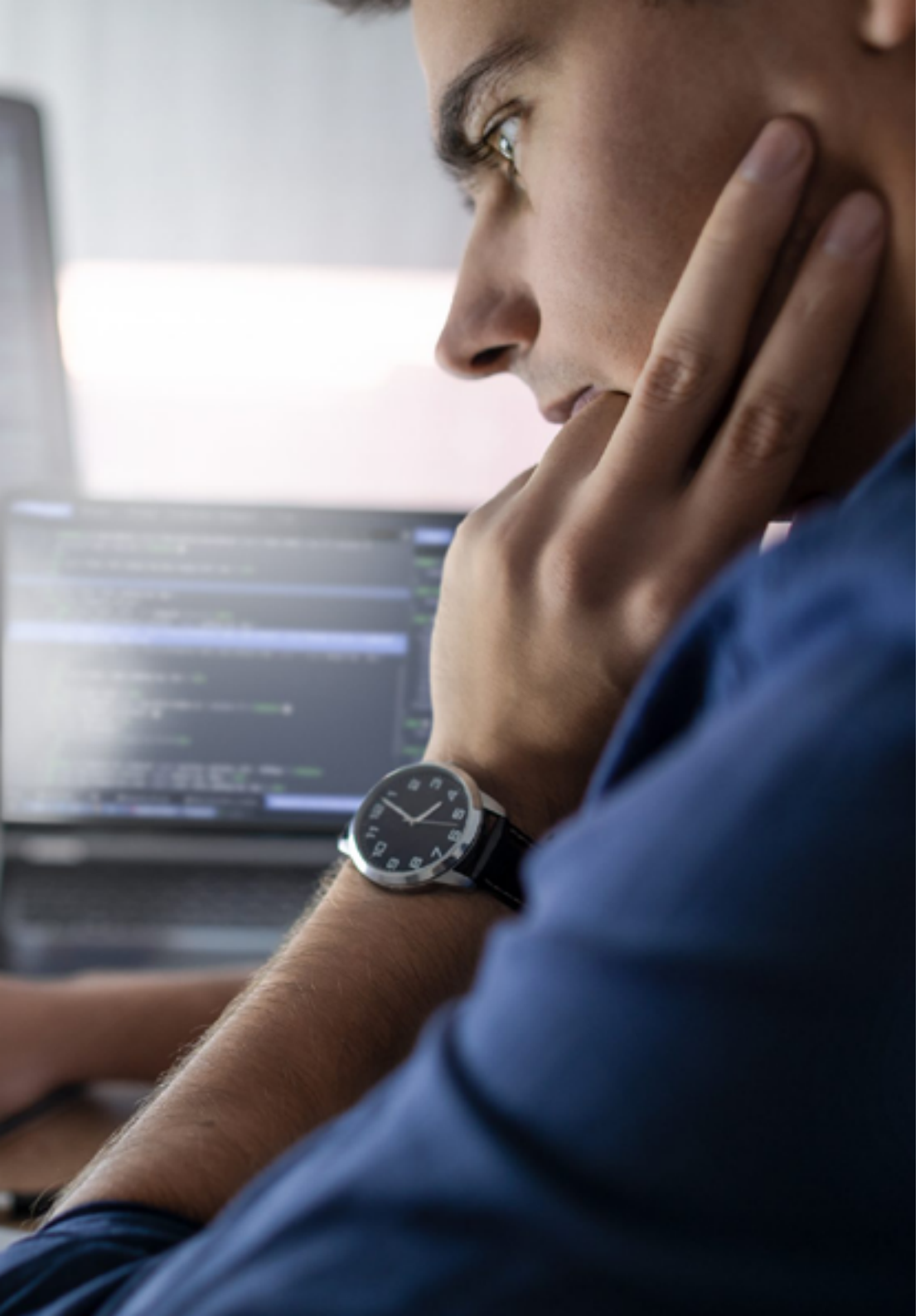
- مدير مشروع في الأمن الإلكترونى. Entelgy Innotec Security
- مستشار الأمن السيبراني. Entelgy
- محلل أمن المعلومات Innovery España
- محلل أمن المعلومات. atos
- بكالوريوس في الهندسة التقنية في أنظمة الكمبيوتر من جامعة قرطبة
- درجة الماجستير في إدارة أمن المعلومات من جامعة البوليتكنيك في مدريد
- شهادة ITIL v4 التأسيسية في إدارة خدمات تكنولوجيا المعلومات. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

د. Rodríguez Peinado, Antonio

- مهندس الحلول السحابية الرئيسي لشركة أوراكل Oracle
- منظم مشارك في ملتقى مطوري ملقة للمطورين
- مستشار متخصص في مجموعة سوبرا جروب وإيفريس
- قائد فريق في System Dynamics
- مطور برمجيات في شركة SGO للبرمجيات
- ماجستير في الأعمال الإلكترونية من كلية La Salle لإدارة الأعمال
- شهادة الدراسات العليا في تكنولوجيا ونظم المعلومات من المعهد الكاتالوني للتكنولوجيا
- بكالوريوس في هندسة الاتصالات من جامعة البوليتكنيك كاتالونيا

د. del Valle Arias, Jorge

- Smart City Solutions & Software Business Development Manager España. Itron، Inc Consultor IoT
- مدير أعمال إنترنت الأشياء المؤقتIoT. TCOMET
- رئيس وحدة أعمال إنترنت الأشياء IoT، وحدة أعمال الصناعة 4.0. Diode España
- مدير مبيعات المنطقة لإنترنت الأشياء IoT والاتصالات. Aicox Soluciones
- المدير الفني ومدير تطوير الأعمال (CTO) ومدير تطوير الأعمال Consultoría TELYC
- المؤسس والرئيس التنفيذي لشركة Sensor Intelligence
- رئيس العمليات والمشاريع. codio
- مدير العمليات في Codium Networks
- كبير مهندسي تصميم الأجهزة والبرامج الثابتة. AITEMIN
- الرئيس الإقليمي لتخطيط وتحسين الترددات اللاسلكية - شبكة LMDS 3.5 جيجا هرتز clearwire
- مهندس اتصالات من الجامعة البوليتكنيك بمدريد
- ماجستير في إدارة الأعمال التنفيذية من كلية الدراسات العليا الدولية في La Salle في مدريد
- ماجيستير في الطاقات المتجددة. CEPYME



أ. García Fernández, Juan Luis

- مدير المنتجات القائمة على Blockchain في Open Canarias
- مدير تطوير عمليات Blockchain DevOps Alastria
- مدير تكنولوجيا مستوى الخدمة في سانتاندير إسبانيا
- مدير تطوير تطبيقات الهاتف المحمول Tinkerlink في Cronos Telecom
- مدير تكنولوجيا إدارة خدمات تكنولوجيا المعلومات في Barclays Bank España
- شهادة في هندسة الحاسب الآلي من جامعة UNED
- التخصص في Deep Learning في DeepLearning.ai

د. Jurado Jabonero, Lorena

- رئيسة أمن المعلومات (CISO) في شركة Grupo Pascual
- مديرة الأمن السيبراني في KPMG إسبانيا
- استشارية إدارة ومراقبة عمليات تكنولوجيا المعلومات ومشاريع البنية التحتية والرقابة عليها في Bankia
- مهندسة أدوات التشغيل في Dalkia
- مطورة في مجموعة Grupo Banco Popular
- مطورة تطبيقات في جامعة البوليتكنيك في مدريد
- بكالوريوس في هندسة الحاسوب من جامعة Alfonso X el Sabio
- مهندسة تقني في إدارة الكمبيوتر من جامعة البوليتكنيك في مدريد.مهندس معتمد في حلول خصوصية البيانات (CDPSE) من ISACA

أ. Ortega, Octavio

- أخصائي التسويق وتطوير الويب
- مبرمج تطبيقات مستقل ومطور ويب مستقلFreelance
- Chief Operating للعمليات في Smallsquid SL
- مسؤول التجارة الإلكترونية فيOrtega y Serrano
- محاضر في دورات شهادة الاحتراف في الحاسب الآلي والاتصالات
- مدرس دورات أمن الحاسب الآلي
- متخرج في علم النفس من جامعة كاتالونيا المفتوحة
- فني جامعي عالي في تحليل البرمجيات وتصميمها وحلولهاSoftware
- تقني جامعي عالي في البرمجة المتقدمة

أ. Simarro Ruiz, Mario

- محامي خبير في تكنولوجيا المعلومات والاتصالات وحماية البيانات في مكتب Martínez-Echevarría للمحامين
- المسؤول القانوني عن Branddocs SL
- محلل مخاطر قطاع الشركات الصغيرة والمتوسطة في BBVA
- أستاذ في الدراسات العليا المتعلقة بالقانون
- بكالوريوس في الحقوق من جامعة Rey Juan Carlos
- بكالريوس في إدارة الأعمال والإدارة من جامعة Rey Juan Carlos
- درجة الماجستير في التكنولوجيات الجديدة والإنترنت والقانون السمعي البصري من مركز للدراسات الجامعيه Villanueva

05

الهيكل والمحتوى

تم تنظيم MBA في إدارة الأمن السيبراني المتقدم في 10 وحدات متخصصة تتيح للمتخصص دراسة جوانب متعمقة مثل التعريف الرقمي، وأنظمة التحكم في الوصول، وبنية أمن المعلومات، وهيكلية مجال الأمن، وأنظمة إدارة أمن المعلومات في الاتصالات وتشغيل البرمجيات أو تطوير خطة استمرارية الأعمال المرتبطة بالأمن. سيمنح ذلك عالم الحاسوب فهماً شاملاً لجميع القضايا ذات الصلة بالأمن السيبراني اليوم.

لن تجد محتوى أكثر اكتمالاً وابتكارًا من هذا المحتوى
المتخصص في إدارة الأمن السيبراني المتقدم"

الوحدة 1. السلامة في التصميم وتطوير الأنظمة

1.1. نظم المعلومات
1.1.1. مجالات نظام المعلومات
2.1.1. مكونات نظام المعلومات
3.1.1. أنشطة نظام المعلومات
4.1.1. دورة حياة نظام المعلومات
5.1.1. موارد نظام المعلومات
2.1. أنظمة المعلومات الأنماط
1.2.1. أنواع نظم المعلومات
1.1.2.1. إدارة الأعمال
2.1.2.1. الاستراتيجية
3.1.2.1. حسب نطاق التطبيق
4.1.2.1. محددة
2.2.1. نظم المعلومات أمثلة حقيقية
3.2.1. تطور نظم المعلومات :مراحل
4.2.1. منهجيات نظم المعلومات
3.1. أمان نظم المعلومات. الآثار القانونية "
1.3.1. الدخول الى البيانات
2.3.1. التهديدات الأمنية: الثغرات الأمنية
3.3.1. الآثار القانونية: الجرائم الجنائية
4.3.1. إجراءات صيانة نظام المعلومات
4.1. أمان نظام المعلومات. بروتوكولات الأمن
1.4.1. أمان نظام المعلومات
1.1.4.1. نزاهة
2.1.4.1. السرية
3.1.4.1. التوفر
4.1.4.1. المصادقة
2.4.1. خدمات أمنية
3.4.1. بروتوكولات أمن المعلومات. الأنماط
4.4.1. حساسية نظام المعلومات
5.1. الأمن في نظم المعلومات. تدابير وأنظمة مراقبة الدخول
1.5.1. إجراءات السلامة
2.5.1. نوع التدابير الاحتياطية
1.2.5.1. الوقاية
2.2.5.1. الكشف
3.2.5.1. التصحيح
3.5.1. أنظمة التحكم في الدخول. الأنماط
4.5.1. علم التشفير
6.1. أمن الشبكات والإنترنت
1.6.1. جدران الحماية
2.6.1. التعريف الرقمي
3.6.1. الفيروسات والديدان
4.6.1. القرصنة Hacking
5.6.1. أمثلة وحالات حقيقية
7.1. الجريمة الإلكترونية
1.7.1. الجريمة الإلكترونية
2.7.1. الجريمة الإلكترونية الأنماط
3.7.1. الجريمة الإلكترونية الهجوم الأنماط
4.7.1. حالة الواقع الافتراضي
5.7.1. لمحات عن الجناة والضحايا. تجريم الجريمة
6.7.1. الجريمة الإلكترونية أمثلة وحالات حقيقية
8.1. الخطة الأمنية لنظام المعلومات
1.8.1. خطة الأمن الأهداف
2.8.1. خطة الأمن التخطيط
3.8.1. خطة المخاطر. التحليلات
4.8.1. سياسات الأمن التنفيذ في المنظمة
5.8.1. خطة الأمن التنفيذ في المنظمة
6.8.1. الإجراءات الأمنية الأنواع
7.8.1. خطة الأمن الأمثلة

9.1. خطة الطوارئ
1.9.1. خطة الطوارئ المهام
2.9.1. خطة الطوارئ العناصر والأهداف
3.9.1. خطة الطوارئ في المنظمة. التنفيذ
4.9.1. خطة الطوارئ الأمثلة
10.1. حوكمة أمن نظم المعلومات
1.10.1. تنظيمات قانونية
2.10.1. المعايير
3.10.1. الشهادات:
4.10.1. التقنيات

الوحدة 2. هياكل ونماذج أمن المعلومات

1.2. بنية أمن المعلومات
1.1.2. SGSI/PDS
2.1.2. التوافق الاستراتيجي
3.1.2. إدارة المخاطر
4.1.2. قياس الأداء
2.2. نماذج أمن المعلومات
1.2.2. استناداً إلى السياسات الأمنية
2.2.2. استنادًا إلى أدوات الحماية
3.2.2. قائمة على الفريق
3.2. نموذج الأمن. المكونات الرئيسية
1.3.2. تعريف المخاطر
2.3.2. تعريف الضوابط
3.3.2. التقييم المستمر لمستويات المخاطر
4.3.2. خطة التوعية للموظفين والموردين والشركاء وغيرهم.
4.2. عمليات ادارة المخاطر
1.4.2. تحديد الأصول
2.4.2. الاستجابة للتهديد
3.4.2. تقييم المخاطر
4.4.2. تحديد أولويات الضوابط
5.4.2. إعادة التقييم والمخاطر المتبقية
5.2. العمليات التجارية وأمن المعلومات
1.5.2. عمليات الأعمال
2.5.2. تقييم المخاطر بناءً على معايير العمل
3.5.2. تحليل أثر الأعمال
4.5.2. العمليات التجارة وامن المعلومات
6.2. عملية التحسين المستمر
1.6.2. دورة الحياة Deming
1.1.6.2. للتخطيط
2.1.6.2. الفعل
3.1.6.2. تحقق
4.1.6.2. الفعل
7.2. معماريات الأمن
1.7.2. اختيار التقنيات وتجانسها
2.7.2. إدارة الهوية المصادقة
3.7.2. إدارة الوصول. الإذن
4.7.2. أمن البنية التحتية للشبكة
5.7.2. تقنيات وحلول التشفير
6.7.2. أمن المعدات الطرفية (EDR)
8.2. الإطار التنظيمي
1.8.2. اللوائح القطاعية
2.8.2. الشهادات:
3.8.2. التشريع
9.2. معيار ISO 10072
1.9.2. التنفيذ
2.9.2. الشهادات
3.9.2. عمليات التدقيق واختبارات الاختراق
4.9.2. إدارة المخاطر
5.9.2. تصنيف المعلومات
10.2. تشريعات الخصوصية. RGPD GDPR
1.10.2. نطاق اللائحة العامة لحماية البيانات (RGPD)
2.10.2. بيانات شخصية
3.10.2. الأدوار في معالجة البيانات الشخصية
4.10.2. حقوق ARCO
5.10.2. المهام El DPO

الوحدة 3. إدارة الأمن IT

1.3. إدارة الأمن
1.1.3. العمليات الأمنية
2.1.3. الجوانب القانونية والتنظيمية
3.1.3. مؤهلات العمل
4.1.3. إدارة المخاطر
5.1.3. إدارة الهوية والوصول
2.3. هيكل المنطقة الأمنية. مكتب مدير أمن المعلومات
1.2.3. الهيكل التنظيمي موقع رئيس أمن المعلومات في الهيكلية CISO
2.2.3. خطوط الدفاع
3.2.3. المخطط التنظيمي لمكتب رئيس أمن المعلومات CISO
4.2.3. إدارة الميزانية
3.3. حكومة الأمن
1.3.3. اللجنة الأمنية
2.3.3. لجنة مراقبة المخاطر
3.3.3. لجنة التدقيق
4.3.3. لجنة الأزمات
4.3. الحكومة الأمنية. المهام
1.4.3. السياسات والمعايير
2.4.3. خطة الأمن
3.4.3. لوحات التحكم
4.4.3. التوعية والتدريب
5.4.3. أمن سلسلة التوريد
5.3. العمليات الأمنية
1.5.3. إدارة الهوية والوصول
2.5.3. تكوين قواعد أمان الشبكة. جدران الحماية
3.5.3. إدارة منصة IDS/IPS
4.5.3. فحص الثغرات الأمنية
6.3. إطار عمل الأمن السيبراني. NIST CSF
1.6.3. منهجية NIST
1.1.6.3. تحديد
2.1.6.3. الحماية
3.1.6.3. الكشف
4.1.6.3. رد
5.1.6.3. التعافي
7.3. مركز العمليات الأمنية (SOC). المهام
1.7.3. الحماية Red Team، pentesting، threat intelligence
2.7.3. الكشف SIEM، user behavior analytics، fraud prevention
3.7.3. رد
8.3. التدقيق الأمني
1.8.3. اختبار التطفل
2.8.3. تمارين الربط الشبكي
3.8.3. تدقيق شفرة المصدر. التطوير الآمن
4.8.3. سلامة المكونات (سلسلة توريد البرمجيات)software supply chain
5.8.3. التحليل الجنائي
9.3. الاستجابة للحوادث
1.9.3. تحضير
2.9.3. الكشف والتحليل والإبلاغ
3.9.3. الاحتواء والاستئصال والتعافي
4.9.3. نشاط ما بعد الحادث
1.4.9.3. الاحتفاظ بالأدلة
2.4.9.3. التحليل الجنائي
3.4.9.3. إدارة الثغرات
5.9.3. الإرشادات الرسمية لإدارة الحوادث السيبرانية
10.3. إدارة الثغرات الأمنية
1.10.3. فحص الثغرات الأمنية
2.10.3. تقييم الثغرات الأمنية
3.10.3. تأسيس النظام
4.10.3. نقاط ضعف اليوم صفر. يوم الصفر

الوحدة 4. تحليل المخاطر وبيئة أمن تكنولوجيا المعلومات

1.4. تحليل البيئة
1.1.4. تحليل الموقف التعليمى
1.1.1.4. بيئة VUCA.
1.1.1.1.4. التقلبات
2.1.1.1.4. Incierto
3.1.1.1.4. التعقيدات
4.1.1.1.4. غامضة
2.1.1.4. بيئة BANI.
1.2.1.1.4. هش
2.2.1.1.4. قلق
3.2.1.1.4. غير خطية
4.2.1.1.4. غير مفهوم
2.1.4. تحليل البيئة العامة. PESTEL
1.2.1.4. السياسي
2.2.1.4. اقتصادية
3.2.1.4. اجتماعي
4.2.1.4. التقنيات
5.2.1.4. إيكولوجي / بيئي
6.2.1.4. الشرعية
3.1.4. تحليل الوضع الداخلي. DAFO
1.3.1.4. الأهداف
2.3.1.4. التهديدات
3.3.1.4. الفرص
4.3.1.4. نقاط القوة
2.4. المخاطر وعدم اليقين
1.2.4. المخاطر
2.2.4. إدارة المخاطر
3.2.4. معايير إدارة المخاطر
3.4. ISO 00103: 8102 مراجعة إدارة الجودة
1.3.4. عنصر
2.3.4. البداية
3.3.4. الإطار المرجعي
4.3.4. العملية
4.4. منهجية تحليل وإدارة مخاطر نظم المعلومات (MAGERIT)
1.4.4. منهجية MAGERIT
1.1.4.4. الأهداف
2.1.4.4. منهج
3.1.4.4. العوامل
4.1.4.4. التقنيات
5.1.4.4. الأدوات المتاحة (PILAR)
5.4. نقل المخاطر السيبرانية
1.5.4. نقل المخاطر
2.5.4. المخاطر السيبرانية. الأنماط
3.5.4. التأمين ضد المخاطر السيبرانية
6.4. منهجيات مرنة لإدارة المخاطر
1.6.4. المنهجيات الرشيقة
2.6.4. Scrum لإدارة المخاطر
3.6.4. AGILE Risk Management
7.4. تقنيات إدارة المخاطر
1.7.4. الذكاء الاصطناعي المطبق على إدارة المخاطر
2.7.4. Blockchain والتشفير. طرق الحفاظ على القيمة
3.7.4. الحوسبة الكمية الفرصة أو التهديد
8.4. تخطيط مخاطر تكنولوجيا المعلومات على أساس المنهجيات الرشيقة
1.8.4. تمثيل الاحتمالية والتأثير في البيئات الرشيقة
2.8.4. المخاطر كتهديد للقيمة
3.8.4. إعادة التطوير في إدارة المشاريع الرشيقة والعمليات القائمة على مؤشرات الأداء الرئيسية

9.4. Risk في إدارة المخاطر
1.9.4. Risk driven
2.9.4. Risk في إدارة المخاطر
3.9.4. تطوير نموذج لإدارة الأعمال قائم على المخاطر
10.4. الابتكار والتحول الرقمي في إدارة مخاطر تكنولوجيا المعلومات
1.10.4. الإدارة الرشيقة للمخاطر كمصدر للابتكار في الأعمال التجارية
2.10.4. تحويل البيانات إلى معلومات مفيدة في اتخاذ القرار
3.10.4. نظرة شمولية للمؤسسة من خلال المخاطر

الوحدة 5. التشفير في تكنولوجيا المعلومات

1.5. علم التشفير
1.1.5. علم التشفير
2.1.5. أساسيات حسابية
2.5. علم التشفير
1.2.5. علم التشفير
2.2.5. تحليل الشفرات
3.2.5. إخفاء المعلومات وتحليل إخفاء المعلومات
3.5. بروتوكولات التشفير
1.3.5. الكتل الأساسية
2.3.5. البروتوكولات الأساسية
3.3.5. البروتوكولات الوسيطة
4.3.5. البروتوكولات المتقدمة
5.3.5. البروتوكولات الخارجية
4.5. تقنيات التشفير
1.4.5. طول المفتاح
2.4.5. الإدارة الرئيسية
3.4.5. أنواع الخوارزميات
4.4.5. ملخص الوظائف. تجزئة
5.4.5. مولدات الأرقام العشوائية الزائفة
6.4.5. استخدام الخوارزميات

5.5. التشفير المتماثل
1.5.5. شفرات التشفير المجمعة
2.5.5. (DES (Data Encryption Standard
3.5.5. خوارزمية 4RC
4.5.5. (AES (Advanced Encryption Standard
5.5.5. مزيج من شفرات الكتل
6.5.5. اشتقاق المفتاح
6.5. التشفير غير المتماثل
1.6.5. Diffie-Hellman
2.6.5. DSA (خوارزمية التوقيع الرقمي)
3.6.5. (RSA (Rivest, Shamir y Adleman
4.6.5. المنحنى البيضاوي
5.6.5. التشفير غير المتماثل الأنماط
7.5. شهادات رقمية
1.7.5. التوقيع الرقمي
2.7.5. شهادات 905X
3.7.5. البنية التحتية للمفاتيح العامة (PKI)
8.5. التنفيذ
1.8.5. Kerberos
2.8.5. IBM CCA
3.8.5. (Pretty Good Privacy (PGP
4.8.5. ISO Authentication Framework
5.8.5. SSL y TLS
6.8.5. (Tarjetas inteligentes en medios de pago (EMV
7.8.5. بروتوكولات الاتصال الهاتفي عبر الهاتف المحمول
8.8.5. Blockchain

9.5. إخفاء المعلومات
1.9.5. إخفاء المعلومات
2.9.5. تحليل التخفي
3.9.5. تطبيقات واستخدامات
10.5. التشفير الكمي
1.10.5. خوارزميات الكم
2.10.5. حماية الخوارزميات من الحوسبة الكمية
3.10.5. توزيع المفاتيح الكمية

الوحدة 6. إدارة الهوية والوصول في أمن تكنولوجيا المعلومات

1.6. إدارة الهوية والوصول (IAM)
1.1.6. الهوية الرقمية
2.1.6. إدارة الهوية
3.1.6. اتحاد الهويات
2.6. التحكم في الوصول المادي
1.2.6. أنظمة الحماية
2.2.6. أمن المناطق
3.2.6. مرافق الاسترداد
3.6. التحكم في الوصول المنطق
1.3.6. المصادقة: التصنيف
2.3.6. بروتوكولات التوثيق
3.3.6. هجمات المصادقة
4.6. التحكم في الوصول المنطق مصادقة MFA
1.4.6. التحكم في الوصول المنطق مصادقة MFA
2.4.6. كلمة المرور: الأهمية
3.4.6. هجمات المصادقة
5.6. التحكم في الوصول المنطق المصادقة البيومترية
1.5.6. التحكم في الوصول المنطقي. المصادقة البيومترية
1.1.5.6. المصادقة البيومترية المتطلبات
2.5.6. التشغيل
3.5.6. أدوات وتقنيات
6.6. نظام إدارة الشركة
1.6.6. Single sign on
2.6.6. Kerberos
3.6.6. أنظمة AAA
7.6. أنظمة إدارة المصادقة: أنظمة AAA
1.7.6. TACACS
2.7.6. RADIUS
3.7.6. DIAMETER
8.6. خدمات التحكم في الوصول
1.8.6. FW-حائط الحماية من الحرائق FIREWALL
2.8.6. الشبكات الافتراضية الخاصة الافتراضية VPN
3.8.6. IDS- أنظمة الكشف عن التسلل
9.6. أنظمة التحكم في الوصول إلى الشبكة
1.9.6. التحكم في الوصول إلى الشبكة
2.9.6. الهندسة المعمارية والعناصر
3.9.6. التشغيل والتوحيد القياسي
10.6. دخول الشبكات اللاسلكية
1.10.6. أنواع الشبكات اللاسلكية
2.10.6. أمان الشبكة اللاسلكية
3.10.6. هجمات الشبكات اللاسلكية

الوحدة 7. الأمن في الاتصالات وتشغيل البرامج

1.7. أمن الكمبيوتر في الاتصالات وتشغيل البرامج
1.1.7. أمن تكنولوجيا المعلومات
2.1.7. الأمن الإلكترونى
3.1.7. أمان السحابة
2.7. أمن الكمبيوتر في الاتصالات وتشغيل البرامج. الأنماط
1.2.7. الأمن المادي
2.2.7. الأمن المنطقي
3.7. أمن الاتصالات
1.3.7. العناصر الرئيسية
2.3.7. أمن الشبكة
3.3.7. أفضل الممارسات

الوحدة 8. الأمان في البيئات السحابيةCloud

1.8. الأمن في بيئات Cloud Computing
1.1.8. الأمن في بيئات Cloud Computing
2.1.8. الأمن في بيئات Cloud Computing التهديدات والمخاطر الأمنية
3.1.8. الأمن في بيئات Cloud Computing الجوانب الرئيسية للتنفيذ
2.8. أنواع البنية التحتية Cloud
1.2.8. عام
2.2.8. خاص
3.2.8. هجين
3.8. نموذج الإدارة المشتركة
1.3.8. ميزات الأمن التي يديرها البائع
2.3.8. العناصر التي يديرها العميل
3.3.8. تحديد الاستراتيجية الأمنية
4.8. الآليات الوقائية
1.4.8. نظام إدارة الشركة
2.4.8. نظام إدارة التفويض: سياسات الوصول
3.4.8. أنظمة الإدارة الرئيسية
5.8. تأمين الأنظمة
1.5.8. التأمين أنظمة التخزين
2.5.8. حماية أنظمة قواعد البيانات
3.5.8. تأمين البيانات أثناء النقل
6.8. حماية البنية التحتية
1.6.8. تصميم الشبكة الآمنة وتنفيذها
2.6.8. أمن موارد الحوسبة
3.6.8. أدوات وموارد لحماية البنية التحتية
7.8. الكشف عن التهديدات والهجمات
1.7.8. أنظمة التدقيق وا Logging والمراقبة
2.7.8. أنظمة الفعاليات والإنذار
3.7.8. أنظمة SIEM
4.7. الذكاء السيبراني
1.4.7. الهندسة الاجتماعية
2.4.7. Deep web
3.4.7. Phishing
4.4.7. البرمجيات الخبيثة
5.7. التطوير الآمن في الاتصالات وتشغيل البرامج
1.5.7. التطوير الآمن بروتوكول HTTP
2.5.7. التطوير الآمن دورة الحياة
3.5.7. التطوير الآمن أمان PHP
4.5.7. التطوير الآمن أمان NET
5.5.7. التطوير الآمن أفضل الممارسات
6.7. أنظمة إدارة أمن معلومات الاتصالات وتشغيل البرمجيات
1.6.7. GDPR
2.6.7. CUGBP Elav-like family member 12072
3.6.7. ISO 81/71072
7.7. تكنولوجيا SIEM
1.7.7. تكنولوجيا SIEM
2.7.7. تشغيل SOC
3.7.7. بائعو SIEM
8.7. دور الأمن في التعبير عن الذات
1.8.7. الأدوار في المنظمات
2.8.7. دور متخصصي إنترنت الأشياءIoT في الشركات
3.8.7. الشهادات المعترف بها في السوق
9.7. التحليل الجنائي
1.9.7. التحليل الجنائي
2.9.7. التحليل الجنائي المنهجية
3.9.7. التحليل الجنائي الأدوات والتنفيذ
10.7. الأمن السيبراني اليوم
1.10.7. الهجمات الرئيسية
2.10.7. توقعات التوظيف
3.10.7. التحديات

8.8. الاستجابة للحوادث
1.8.8. خطة الاستجابة للحوادث
2.8.8. استمرارية الأعمال
3.8.8. تحليل الطب الشرعي ومعالجة الحوادث من نفس الطبيعة
9.8. الأمن في السحابة العامةClouds
1.9.8. AWS(خدمات أمازون على الويب)
2.9.8. Microsoft Azure
3.9.8. Google GCP
4.9.8. Oracle Cloud
10.8. اللوائح التنظيمية والامتثال
1.10.8. الامتثال للوائح السلامة
2.10.8. إدارة المخاطر
3.10.8. أشخاص الإجراءات في المنظمات

الوحدة 9. أمن اتصالات أجهزة إنترنت الأشياء

1.9. من القياس عن بُعد إلى إنترنت الأشياءIoT
1.1.9. القياس عن بُعد
2.1.9. الاتصال من آلة إلى آلة M2M
3.1.9. إضفاء الطابع الديمقراطي على القياس عن بُعد
2.9. النموذج المرجعي
1.2.9. النموذج المرجعي
2.2.9. بنية إنترنت الأشياء المبسطةIoT
3.9. الثغرات الأمنية في إنترنت الأشياءIoT
1.3.9. أجهزة إنترنت الأشياء.
2.3.9. أجهزة إنترنت الأشياء. دراسات حالة الاستخدام
3.3.9. أجهزة إنترنت الأشياء. نقاط الضعف
4.9. اتصال إنترنت الأشياء IoT
1.4.9. شبكات PAN و LAN و WAN
2.4.9. تقنيات لاسلكية غير إنترنت الأشياء IoT
3.4.9. التقنيات اللاسلكيةLPWAN
5.9. تكنولوجيا LPWAN
1.5.9. المثلث الحديدي لشبكات LPWAN
2.5.9. نطاقات التردد الحر مقابل الفرق الموسيقية المرخصة
3.5.9. خيارات تقنية LPWAN
6.9. تقنية LoRaWAN
1.6.9. تقنية LoRaWAN
2.6.9. حالات الاستخدام LoRaWAN المنظومة
3.6.9. الأمن في LoRaWAN
7.9. تقنية Sigfox
1.7.9. تقنية Sigfox
2.7.9. حالات الاستخدام Sigfox. المنظومة
3.7.9. الأمن في Sigfox.
8.9. تقنية إنترنت الأشياء الخلوية IoT
1.8.9. تقنية إنترنت الأشياء الخلوية (LTE-Mg NB-IoT)
2.8.9. حالات استخدام إنترنت الأشياء الخلوي. المنظومة
3.8.9. الأمن في الخلايا إنترنت الأشياء IoT
9.9. تقنية WiSUN
1.9.9. تقنية WiSUN
2.9.9. حالات الاستخدام المنظومة
3.9.9. أمن WiSUN
10.9. تقنيات IoT الأخرى
1.10.9. تقنيات IoT الأخرى
2.10.9. حالات الاستخدام والنظام البيئي لتقنيات إنترنت الأشياء الأخرى
3.10.9. الأمن في تقنيات إنترنت الأشياء الأخرى

الوحدة 10. خطة استمرارية الأعمال المرتبطة بالأمن

1.10. خطط استمرارية الأعمال
1.1.10. خطط استمرارية الأعمال (PCN)
2.1.10. خطة استمرارية الأعمال (PCN). الجوانب الرئيسية
3.1.10. خطة استمرارية الأعمال (PCN) لتقييم الشركة
2.10. المقاييس في خطة استمرارية الأعمال
1.2.10. Recovery Time Objective (RTO) y Recovery Point Objective RPO
2.2.10. الحد الأقصى للوقت المسموح به (MTD)
3.2.10. الحد الأدنى لمستويات الاسترداد (ROL)
4.2.10. هدف نقطة الاسترداد (RPO)
3.10. مشاريع الاستمرارية. الأنماط
1.3.10. خطة استمرارية الأعمال
2.3.10. خطة استمرارية تكنولوجيا المعلومات والاتصالات (ICTCSP)
3.3.10. خطة التعافي من الكوارث (DRP)
4.10. إدارة المخاطر المرتبطة بخطة استمرارية تصريف الأعمال
1.4.10. تحليل أثر الأعمال
2.4.10. فوائد تنفيذ عن PCN
3.4.10. العقلي القائم على المخاطر
5.10. دورة حياة خطة استمرارية الأعمال
1.5.10. المرحلة 1: تحليل التنظيم
2.5.10. المرحلة 2: تحديد استراتيجية المستمر
3.5.10. المرحلة 3: الاستجابة للطوارئ
4.5.10. المرحلة 4: الاختبار والصيانة والتدقيق
6.10. مرحلة التحليل التنظيمي لخطة استمرارية تصريف الأعمال
1.6.10. تحديد العمليات التي تقع في نطاق خطة استمرارية تصريف الأعمال
2.6.10. تحديد مجالات العمل الحرجة
3.6.10. تحديد التبعيات بين المجالات والعمليات
4.6.10. تحديد أفضل التقنيات المتاحة في أفضل التقنيات المتاحة
5.6.10. الإنجازات وضع خطة
7.10. مرحلة تحديد استراتيجية الاستمرارية في خطة استمرارية تصريف الأعمال
1.7.10. الأدوار في مرحلة تحديد الاستراتيجية
2.7.10. المهام في مرحلة تحديد الاستراتيجية
3.7.10. الإنجازات
8.10. مرحلة الاستجابة للطوارئ في خطة استمرارية تصريف الأعمال
1.8.10. الأدوار في مرحلة الاستجابة
2.8.10. المهام في هذه المرحلة
3.8.10. الإنجازات
9.10. مرحلة اختبار وصيانة ومراجعة خطة استمرارية تصاميم استمرارية الأعمال
1.9.10. الأدوار في مرحلة الاختبار والصيانة والمراجعة
2.9.10. المهام في مرحلة الاختبار والصيانة والإصلاح الشامل
3.9.10. الإنجازات
10.10. معايير ISO المرتبطة بخطط استمرارية الأعمال
1.10.10. ISO 9102:10322
2.10.10. ISO 0202:13322
3.10.10. معايير ISO والمعايير الدولية الأخرى ذات الصلة

الوحدة 11. القيادة والأخلاق والمسؤولية الاجتماعية للشركة

1.11. العولمة والحوكمة
1.1.11. الحوكمة والحوكمة المؤسسية
2.1.11. أساسيات حوكمة الشركات في الشركات
3.1.11. دور مجلس الإدارة في إطار حوكمة الشركات
2.11. القيادة
1.2.11. القيادة. النهج المفاهيمي
2.2.11. القيادة في الشركات
3.2.11. أهمية القائد في إدارة الأعمال
3.11. Cross Cultural Management
1.3.11. مفهوم Cross Cultural Management
2.3.11. مساهمات في معرفة الثقافات الوطنية
3.3.11. إدارة التنوع
4.11. التنمية الإدارية والقيادة
1.4.11. مفهوم التنمية الإدارية
2.4.11. مفهوم القيادة
3.4.11. نظريات القيادة
4.4.11. أساليب القيادة
5.4.11. الذكاء في القيادة
6.4.11. تحديات القائد اليوم

5.11. أخلاقيات العمل
1.5.11. الأخلاق والأخلاقيات
2.5.11. أخلاقيات الأعمال التجارية
3.5.11. القيادة والأخلاقيات في الشركة
6.11. الاستدامة
1.6.11. الاستدامة 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. RSC: المسؤولية الاجتماعية للشركات
2.8.11. القضايا الرئيسية في تنفيذ استراتيجية الإدارة المسؤولة
3.8.11. خطوات تطبيق نظام إدارة المسؤولية الاجتماعية للشركات
4.8.11. أدوات ومعايير المسؤولية الاجتماعية للشركات
9.11. الشركات متعددة الجنسيات وحقوق الإنسان
1.9.11. العولمة والشركات متعددة الجنسيات وحقوق الإنسان
2.9.11. الشركات متعددة الجنسيات مقابل القانون الدولي
3.9.11. الصكوك القانونية للشركات المتعددة الجنسيات فيما يتعلق بحقوق الإنسان
10.11. البيئة القانونية و Corporate Governance
1.10.11. لوائح الاستيراد والتصدير الدولية
2.10.11. الملكية الفكرية والصناعية
3.10.11. قانون العمل الدولي

الوحدة 12. قيادة 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. إنتاجية المواهب وجذبها 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. جدول التدفق النقدى Cash Flow
5.6.13. الجدول الحالي
7.13. الاستراتيجية المالية للشركة
1.7.13. الاستراتيجية المؤسسية ومصادر التمويل
2.7.13. المنتجات المالية لتمويل الأعمال
8.13. التمويل الاستراتيجي
1.8.13. التمويل الذاتي
2.8.13. زيادة الأموال الخاصة
3.8.13. الموارد الهجينة
4.8.13. التمويل عن طريق الوسطاء
9.13. التحليل المالي والتخطيط
1.9.13. تحليل الميزانية العمومية
2.9.13. تحليل قائمة الدخل
3.9.13. 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. مزايا وعيوب التجارة الإلكترونيةEcommerce مقابل التجارة التقليدية

5.14. التسويق الرقمي لتقوية العلامة التجارية
- 1.5.14. استراتيجيات عبر الإنترنت لتحسين سمعة علامتك التجارية
- 2.5.14. Branded Content & Storytelling

6.14. التسويق الرقمي لجذب العملاء والاحتفاظ بهم
- 1.6.14. استراتيجيات الولاء والمشاركة عبر الإنترنت
- 2.6.14. إدارة علاقات الزوار
- 3.6.14. التجزئة المفرطة

7.14. ادارة الحملات الرقمية
- 1.7.14. ما هي الحملة الإعلانية الرقمية؟
- 2.7.14. خطوات إطلاق حملة تسويق عبر الإنترنت
- 3.7.14. أخطاء في الحملات الإعلانية الرقمية

8.14. استراتيجية المبيعات
- 1.8.14. استراتيجية المبيعات
- 2.8.14. طرق البيع

9.14. 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. التواصل والسمعة الرقمية
- 1.10.14. السمعة عبر الانترنت
- 2.10.14. كيفية قياس السمعة الرقمية؟
- 3.10.14. أدوات السمعة عبر الإنترنت
- 4.10.14. تقرير السمعة عبر الإنترنت
- 5.10.14. Branding عبر الإنترنت

الوحدة 15. مدير إدارة

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. التواصل بين الأشخاص
- 2.4.15. مهارات التواصل والتأثير
- 3.4.15. حواجز التواصل

5.15. أدوات. التواصل الشخصية والتنظيمية
1.5.15. التواصل بين الأشخاص
2.5.15. أدوات التواصل بين الأشخاص
3.5.15. التواصل في المنظمات
4.5.15. الأدوات في المنظمة
6.15. 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 والتواصل
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 لتطوير علامتك التجارية الشخصية
2.9.15. قوانين العلامات التجارية الشخصية
3.9.15. أدوات بناء العلامة التجارية الشخصية
10.15. القيادة وإدارة الفرق
1.10.15. القيادة وأساليب القيادة
2.10.15. قدرات القائد والتحديات
3.10.15. إدارة عملية التغيير
4.10.15. إدارة فرق متعددة الثقافات

يتم الجمع بين أفضل أعضاء هيئة التدريس ونظام التدريس المبتكر مع المنهج الدراسي الأكثر اكتمالاً وحداثة: لديك فرصة كبيرة للتقدم كعالم كمبيوتر"

06

المنهجية

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

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

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

منهج دراسة الحالة لوضع جميع محتويات المنهج في سياقها المناسب

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

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

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

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

منهج تعلم مبتكرة ومختلفة

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

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

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

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

منهجية إعادة التعلم *(Relearning)*

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

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

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

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

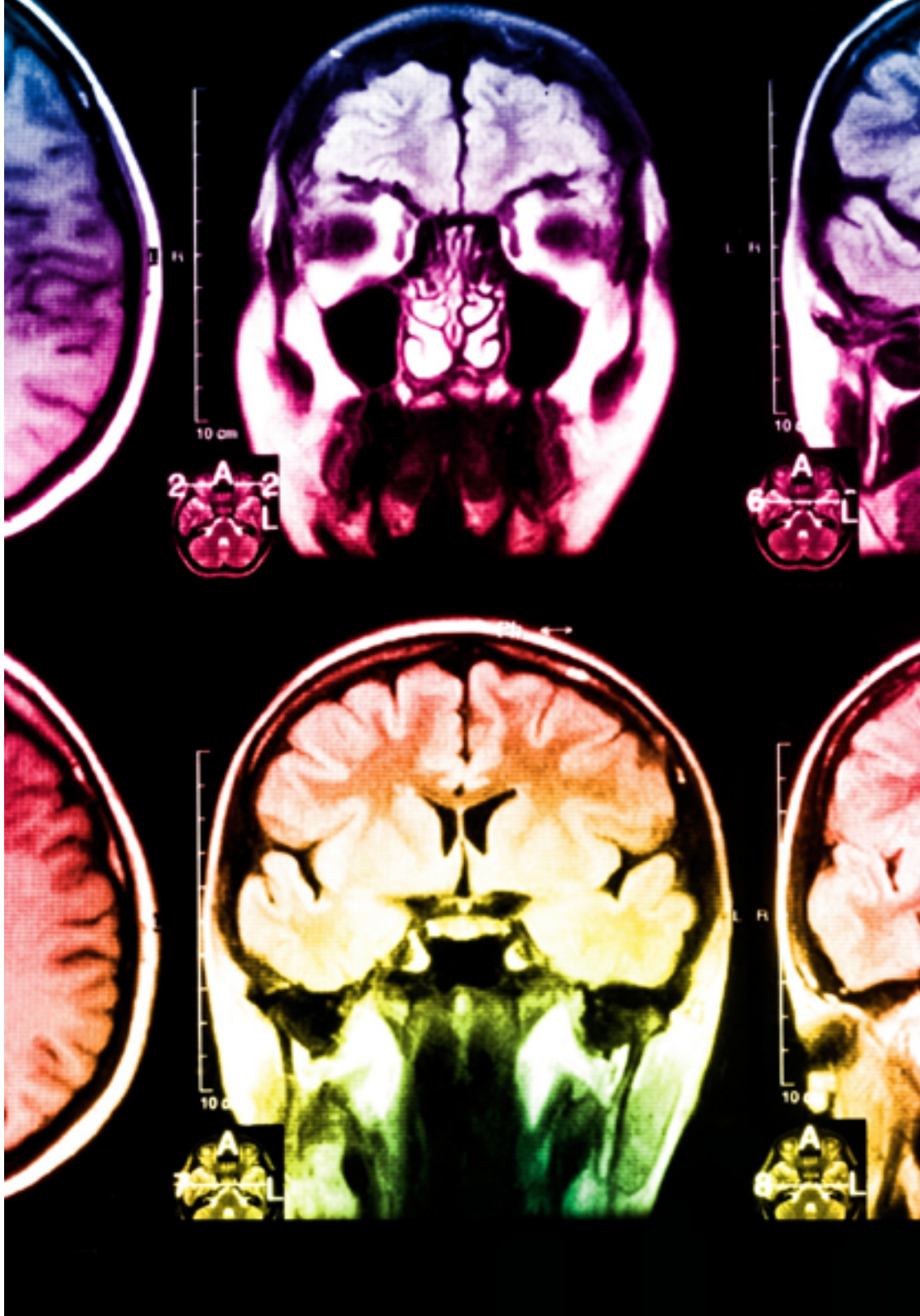
جامعتنا هي الجامعة الوحيدة الناطقة باللغة الإسبانية المصرح لها لاستخدام هذا المنهج الناجح. في عام 2019، تمكنا من تحسين مستويات الرضا العام لطلابنا من حيث (جودة التدريس، جودة المواد، هيكل الدورة، الأهداف..) فيما يتعلق بمؤشرات أفضل جامعة عبر الإنترنت باللغة الإسبانية.

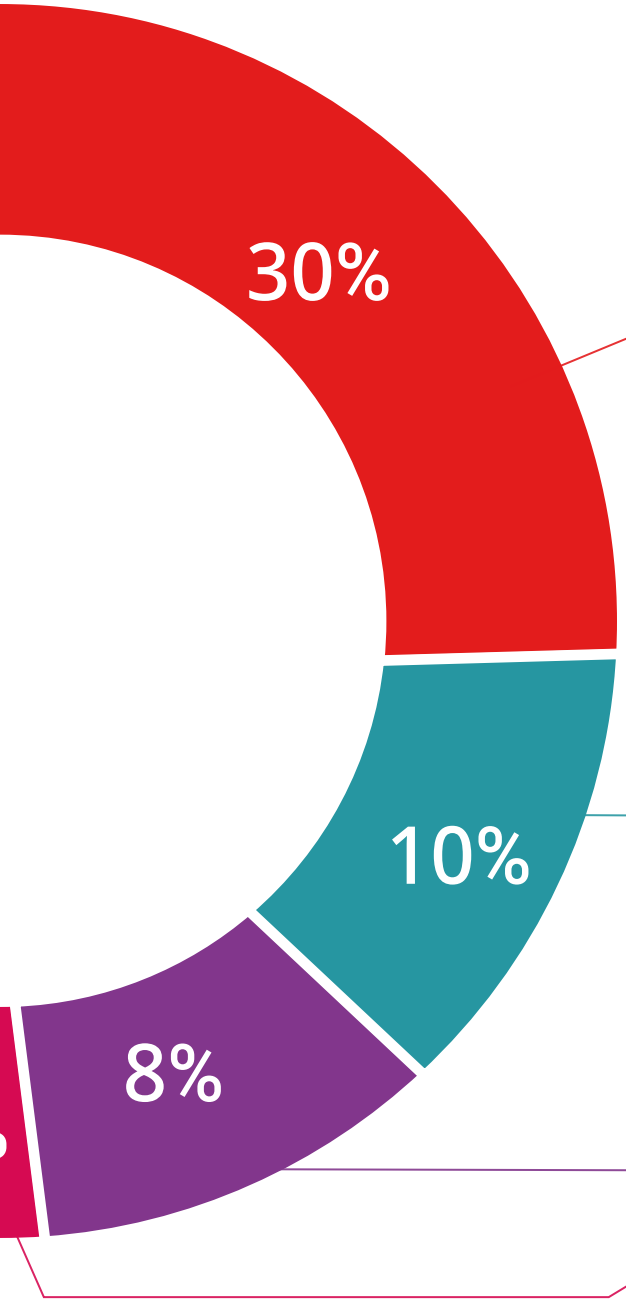
في برنامجنا، التعلم ليس عملية خطية، ولكنه يحدث في شكل لولبي (نتعلّم ثم نطرح ماتعلمناه جانبًا فننساه ثم نعيد تعلمه). لذلك، نقوم بدمج كل عنصر من هذه العناصر بشكل مركزي. باستخدام هذه المنهجية، تم تدريب أكثر من 650000 خريج جامعي بنجاح غير مسبوق في مجالات متنوعة مثل الكيمياء الحيوية، وعلم الوراثة، والجراحة، والقانون الدولي، والمهارات الإدارية، وعلوم الرياضة، والفلسفة، والقانون، والهندسة، والصحافة، والتاريخ، والأسواق والأدوات المالية. كل ذلك في بيئة شديدة المتطلبات، مع طلاب جامعيين يتمتعون بمظهر اجتماعي واقتصادي مرتفع ومتوسط عمر يبلغ 43.5 عاماً.

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

استنادًا إلى أحدث الأدلة العلمية في مجال علم الأعصاب، لا نعرف فقط كيفية تنظيم المعلومات والأفكار والصور والذكريات، ولكننا نعلم أيضًا أن المكان والسياق الذي تعلمنا فيه شيئًا هو ضروريًا لكي نكون قادرين على تذكرها وتخزينها في الحُصين بالمخ، لكي نحتفظ بها في ذاكرتنا طويلة المدى.

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





يقدم هذا البرنامج أفضل المواد التعليمية المُعَدَّة بعناية للمهنيين:

المواد الدراسية

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

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

المحاضرات الرئيسية

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

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

التدريب العملي على المهارات والكفاءات

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

قراءات تكميلية

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

دراسات الحالة (Case studies)

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

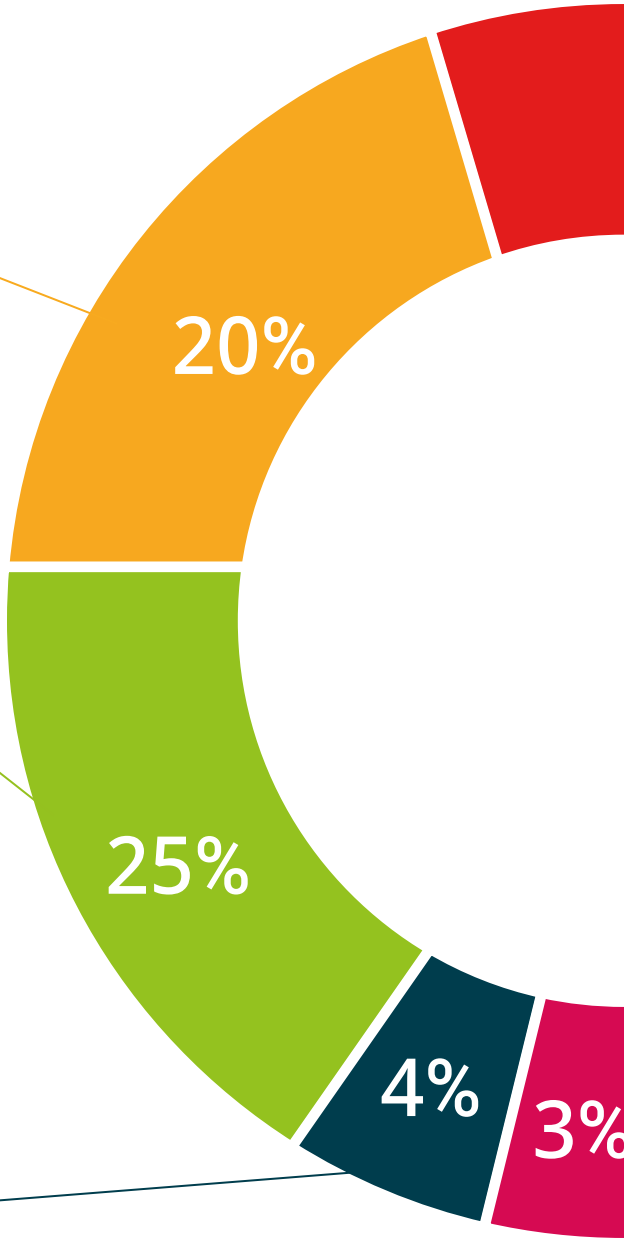
ملخصات تفاعلية

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

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

الاختبار وإعادة الاختبار

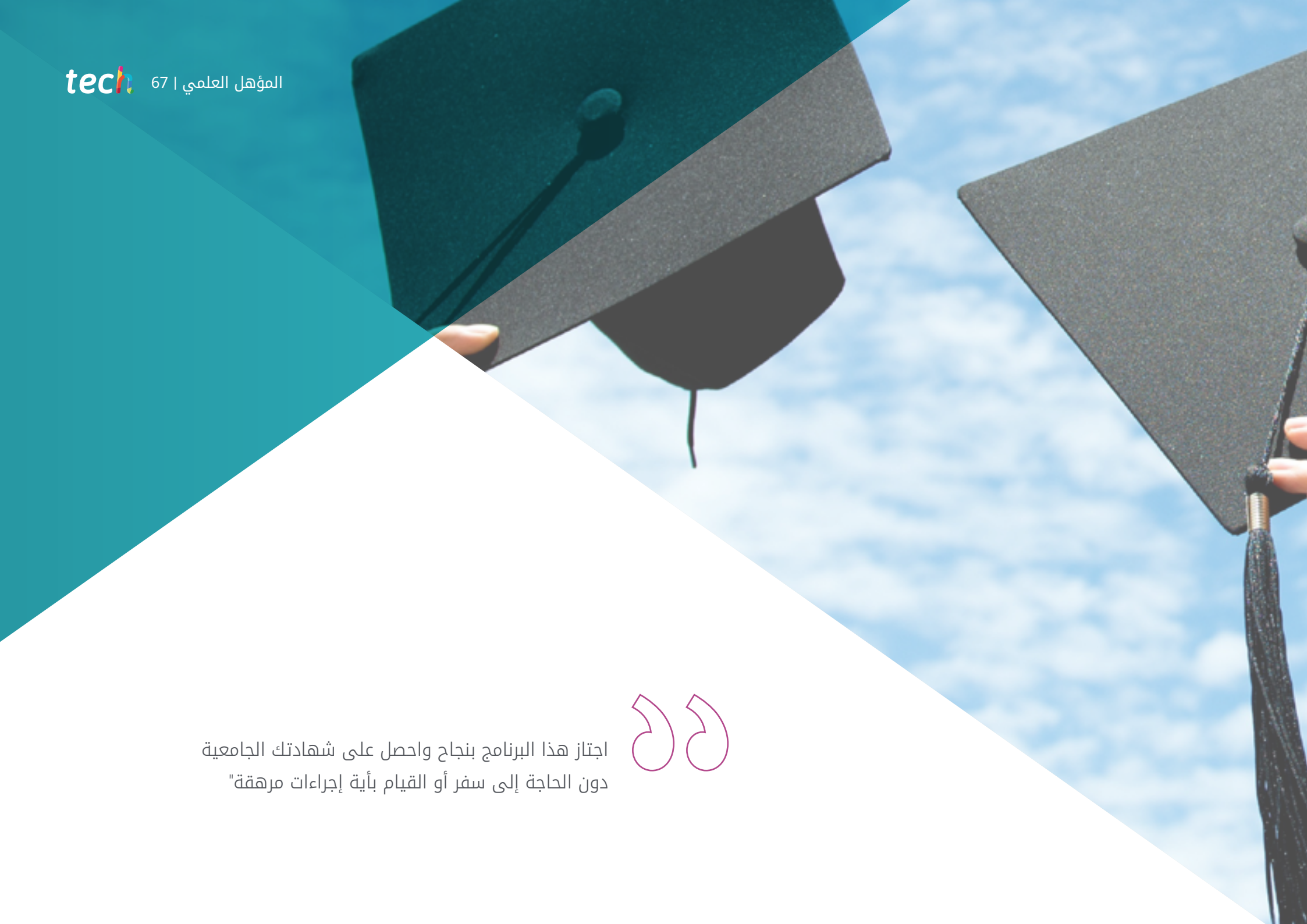
يتم بشكل دوري تقييم وإعادة تقييم معرفة الطالب في جميع مراحل البرنامج، من خلال الأنشطة والتدريبات التقييمية وذاتية التقييم: حتى يتمكن من التحقق من كيفية تحقيق أهدافه.



07

المؤهل العلمي

يضمن ماجستير نصف حضوري في MBA إدارة الأمن السيبراني المتقدم (CISO)، بالإضافة إلى التدريب الأكثر صرامة وحداثة، الحصول على مؤهل الماجستير الخاص الصادر عن TECH الجامعة التكنولوجية.



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

يحتوي هذا **ماجستير نصف حضوري في MBA إدارة الأمن السيبراني المتقدم (CISO)** على البرنامج الأكثر اكتمالاً وحداثة في السوق.

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

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

المؤهل العلمي: **ماجستير نصف حضوري في MBA إدارة الأمن السيبراني المتقدم (CISO)**

اطريقة: **عبر الإنترنت**

مدة: **12 شهر**


tech الجامعة التكنولوجية

شهادة تخرج

هذه الشهادة ممنوحة إلى

لـ

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

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

ماجستير خاص

في

MBA إدارة الأمن السيبراني المتقدم (CISO)

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

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

في تاريخ 17 يونيو 2020

أ. د./ Tere Guevara Navarro
رئيس الجامعة

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


ماجستير خاص MBA إدارة الأمن السيبراني المتقدم (CISO)

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
1º	السلامة في التصميم وتطوير الأنظمة	إجباري	100
1º	هياكل ونماذج أمن المعلومات	إجباري	100
1º	إدارة الأمن IT	إجباري	100
1º	تحليل المخاطر وبيئة أمن تكنولوجيا المعلومات	إجباري	100
1º	التشفير في تكنولوجيا المعلومات	إجباري	100
1º	إدارة الهوية والوصول في أمن تكنولوجيا المعلومات	إجباري	100
1º	الأمن في الاتصالات وتشغيل البرامج	إجباري	100
1º	الأمن في البيئات السحابية	إجباري	100
1º	أمن اتصالات أجهزة إنترنت الأشياء	إجباري	100
1º	خطة استمرارية الأعمال المرتبطة بالأمن	إجباري	100
1º	القيادة والأخلاق والمسؤولية الاجتماعية للشركة	إجباري	100
1º	قيادة الأفراد وإدارة المواهب	إجباري	100
1º	الإدارة الاقتصادية والمالية	إجباري	100
1º	الإدارة التجارية والتسويق الاستراتيجي	إجباري	100
1º	الإدارة التنفيذية (Management)	إجباري	100

tech الجامعة التكنولوجية

أ. د./ Tere Guevara Navarro
رئيس الجامعة

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

الجامعة التيكنولوجية

ماجيستير خاص
MBA إدارة الأمن السيبراني المتقدم (CISO)

- 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 السيبراني المتقدم (CISO)

tech الجامعة التيكنولوجية