ماجستير متقدم

الإدارة العليا في الأمن السيبراني
(CISO، الرئيس التنفيذي لأمن المعلومات)

tech الجامعة التيكنولوجية

الجامعة التيكنولوجية

ماجستير متقدم
الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات)

- طريقة الدراسة: **عبر الإنترنت**
- مدة الدراسة: **2 سنتين**
- المؤهل العلمي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **عبر الإنترنت**

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

الفهرس

01

تقديم البرنامج

لقد أصبح الأمن السيبراني اليوم ركيزة أساسية في حماية الأفراد والشركات من التهديدات الرقمية المتزايدة. لا يركز هذا التخصص على حماية الأنظمة التقنية والمعلومات الهامة للمؤسسات فحسب، بل يركز أيضاً على قيادة تخطيط وتنفيذ ومراقبة الاستراتيجيات الأمنية. بالتالي، فإن هدفها الرئيسي هو تخفيف المخاطر والاستجابة بفعالية للهجمات والحوادث الإلكترونية. تشمل المسؤوليات الرئيسية لمدير الأمن السيبراني تصميم السياسات الأمنية وإدارة المخاطر التكنولوجية وقيادة الفرق المتخصصة. في مواجهة التحديات الناشئة عن التقدم التكنولوجي والرقمنة، صُمم هذا البرنامج خصيصاً لمعالجة هذه القضايا. لا يقتصر تركيز TECH على ضمان الكفاءة في حماية المعلومات فحسب، بل أيضًا على تحديد نقاط الضعف الجديدة وإدارتها. هذا يضع رئيس أمن المعلومات في المرتبة الأولى كأهم عنصر لمرونة أي مؤسسة.

مع TECH، تخصص وكن رائداً في أحد أهم مجالات تكنولوجيا المعلومات"

كان للإدارة العليا للأمن السيبراني دور فعال في ضمان استقرار المؤسسات واستمراريتها في عالم رقمي ومترابط للغاية. من خلال تنفيذ استراتيجيات أمنية قوية واعتماد تقنيات متقدمة، تم الحد من المخاطر ومنع وقوع هجمات كارثية. في القطاعات الحيوية مثل القطاع المصرفي والرعاية الصحية والبنية التحتية العامة، تم تعزيز الأمن من خلال الحوكمة والامتثال، بقيادة قادة متخصصين في هذا المجال.

مكّن هذا النظام المؤسسات من إنشاء بيئات عمل رقمية أكثر أماناً، وبالتالي تعزيز ثقة العملاء والشركاء والمستخدمين. أدت النتائج الناجحة إلى تحقيق وفورات كبيرة تقدر بملايين الدولارات من الخسائر الاقتصادية المحتملة، مع تعزيز ثقافة مؤسسية تكون السلامة فيها أولوية مشتركة. أثبت أيضًا أنه ضروري في حماية الابتكار والسمعة والاستدامة للمؤسسات في مشهد يتطور باستمرار.

تم تصميم برنامج TECH الماجستير المتقدم لتدريب المتخصصين في قيادة الاستراتيجيات الأمنية الفعالة. سيتعلم الطلاب خلال البرنامج بالسرعة التي تناسبهم، مع التركيز على تطوير المهارات الإدارية والرؤية الاستراتيجية للأعمال. بالإضافة إلى ذلك، ستتمكن من الحصول على تخصص متطور يؤهلك للتفوق في مهنة مطلوبة بشدة في السوق العالمية. بفضل شكله المتاح 100% عبر الإنترنت، سيتمكن المشاركون من الجمع بين دراستهم ومسؤوليات عملهم، مما يسمح لهم بالتقدم دون المساس بنشاطهم المهني.

يحتوي هذا **الماجستير المتقدم في الإدارة العليا للأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات)** على البرنامج التعليمي الأكثر اكتمالاً وحداثة في السوق. أبرز خصائصه هي:

- تطوير الحالات العملية التي يقدمها خبراء في نظم المعلومات
- المحتويات الرسومية والتخطيطية والعملية البارزة التي يتم تصورها بها، تجمع المعلومات العلمية والعملية حول تلك التخصصات الأساسية للممارسة المهنية
- التمارين العملية حيث يمكن إجراء عملية التقييم الذاتي لتحسين التعلم
- تركيزه الخاص على المنهجيات المبتكرة في الإدارة العليا للأمن السيبراني(CISO، الرئيس التنفيذي لأمن المعلومات)
- دروس نظرية وأسئلة للخبراء ومنتديات مناقشة حول القضايا المثيرة للجدل وأعمال التفكير الفردية
- توفر المحتوى من أي جهاز ثابت أو محمول متصل بالإنترنت

> يضعك هذا الماجستير المتقدم في طليعة الصناعة ويفتح لك فرصاً مهنية لا حصر لها"

طوّر المهارات التي تحتاجها لمواجهة تحديات المستقبل دون إهمال أنشطتك الحالية"

كن حاميًا للبنى التحتية التكنولوجية مع طريقة إعادة التعلم التي تتكيف مع وتيرة تعلمك.

كن جزءاً من أكبر جامعة رقمية في العالم وتخصص من أي مكان في العالم.

يضم في أعضاء هيئة تدريسه محترفين في مجال الصحافة يصبون في هذا البرنامج خبرة عملهم، بالإضافة إلى متخصصين معترف بهم من الجمعيات المرجعية والجامعات المرموقة.

إن محتوى الوسائط المتعددة الذي تم تطويره باستخدام أحدث التقنيات التعليمية، والذين سيتيح للمهني فرصة للتعلم الموضوعي والسياقي، أي في بيئة محاكاة ستوفر تعليماً غامرًا مبرمجًا للتدريب في مواقف حقيقية.

يركز تصميم هذا البرنامج على التعلم القائم على المشكلات، والذي يجب على الطالب من خلاله محاولة حل الحالات المختلفة للممارسة المهنية التي تُطرَح على مدار هذه الدورة الأكاديمية. للقيام بذلك، المهني سيحصل على مساعدة من نظام فيديو تفاعلي مبتكر من قبل خبراء مشهورين.

02

لماذا تدرس في TECH؟

جامعة TECH هي أكبر جامعة رقمية في العالم. مع وجود قائمة مذهلة تضم أكثر من 14000 برنامج الجامعي بـ 11 لغة، مايجعلها تحتل مكانة رائدة في مجال التوظيف، حيث يبلغ معدل التوظيف فيها 99%. كما أن لديها هيئة تدريس ضخمة تضم أكثر من 6000 أستاذ مشهور عالمياً.

ادرس في أكبر جامعة رقمية في العالم واضمن نجاحك المهني. المستقبل يبدأ من TECH"

أفضل جامعة عبر الإنترنت في العالم وفقًا لمجلة FORBES

أشادت مجلة فوربس المرموقة، المتخصصة في الأعمال والتمويل، بـ TECH ووصفتها بأنها «أفضل جامعة عبر الإنترنت في العالم». وقد أكدت ذلك مؤخرًا في مقال نُشر في نسختها الرقمية، حيث سلطت الضوء على نجاح هذه المؤسسة «بفضل عرضها الأكاديمي، واختيارها لفريقها التدريسي، ومنهجها التعليمي المبتكر الذي يهدف إلى تأهيل مهنيي المستقبل»

أفضل هيئة تدريس دولية من النخبة

تضم هيئة التدريس في TECH أكثر من 000, أستاذ من أعلى مستويات التقدير الدولي. أساتذة وباحثون وكبار المديرين التنفيذيين من شركات متعددة الجنسيات، من بينهم Isaiah Covington، مدرب الأداء في فريق Boston Celtics، Magda Romanskag، الباحثة الرئيسية في Harvard MetaLAB، Egacio Wistumbag، رئيس قسم علم الأمراض الجزيئية الانتقالية في مركز MD Anderson لعلاج السرطان، و D.W. Pine، المدير الإبداعي لمجلة TIME، وغيرهم.

أكبر جامعة رقمية في العالم

جامعة TECH أكبر جامعة رقمية في العالم. نحن أكبر نطاق تعليمية، بأفضل وأوسع قائمة برامج تعليمية رقمية، مائة في المئة عبرالانترنت وتغطي الغالبية العظمى من شتى مجالات المعرفة. نحن نقدم أكبر عدد من المؤهلات العلمية الجامعية الخاصة والمعتمدة في الدراسات العليا عبرالأنترنت وكذلك في البكالوريوس الجامعي. أجمالا، أكثر من 14000 مؤهل جامعي، بإحدى عشر لغة مختلفة، تجعلنا أكبر نطاق تعليمية في العالم.

أكثر الخطط الدراسية شمولاً في المشهد الجامعي

توفر TECH أكثر الخطط الدراسية تكاملاً في المشهد الجامعي، مع مناهج تشمل المفاهيم الأساسية وأحدث التطورات العلمية في مجالاتها التخصصية. بالإضافة إلى ذلك، يتم تحديث هذه البرامج باستمرار لضمان تزويد الطلاب بأحدث المعارف الأكاديمية والمهارات المهنية الأكثر طلبًا. وبذلك، تمنح شهادات الجامعة لخريجيها ميزة كبيرة لدفع مسيرتهم المهنية نحو النجاح.

أسلوب تعليمي فريد

تعد TECH أول جامعة تطبق منهجية Relearning في جميع برامجها الأكاديمية.. ويُعتبر هذا النهج أفضل أسلوب تعليمي عبر الإنترنت، حيث حصل على شهادات جودة أكاديمية دولية معتمدة من وكالات تعليمية مرموقة. علاوة على ذلك، يُكمل هذا النموذج الأكاديمي المتطور بـ"منهجية الحالة"، مما يشكل استراتيجية تعليمية رقمية فريدة من نوعها. كما تعتمد الجامعة موارد تعليمية مبتكرة تشمل مقاطع فيديو تفصيلية، وإنفوجرافيك، وملخصات تفاعلية.

الجامعة الافتراضية الرسمية للرابطة الوطنية لكرة السلة NBA

جامعة TECH هي الجامعة الرسمية عبر الإنترنت للـNBA وبفضل شراكتها مع أكبر دوري لكرة السلة في العالم، تقدم برامج جامعية حصرية لطلابها، بالإضافة إلى مجموعة واسعة من الموارد التعليمية التي تركز على قطاع أعمال الرابطة ومجالات أخرى في صناعة الرياضة. كل برنامج مصمم بمحتوى أكاديمي فريد، ويشمل محاضرات يقدمها متحدثون متميزون، وهم خبراء رياضيون بارزون يشاركون خبراتهم حول الموضوعات الأكثر أهمية.

الريادة في التوظيف

نجحت TECH في أن تصبح الجامعة الرائدة في توظيف الخريجين، حيث يحصل 99% من طلابها على وظيفة في مجالهم الأكاديمي خلال أقل من عام من التخرج. كما يتمكن عدد كبير منهم من تحسين مسارهم المهني فور الانتهاء من برامجهم الدراسية. ويعود هذا النجاح إلى منهجية تعليمية تركز على اكتساب المهارات العملية، وهي عنصر أساسي لضمان التفوق المهني في سوق العمل.

99%
Garantía de máxima empleabilidad

4.9/5
global score

Universidad online oficial de la NBA

Google Partner
PREMIER 2023

الجامعة الأعلى تصنيفاً على مستوى العالم قبل طلابها

حصلت TECH على لقب الجامعة الأعلى تقييمًا عالميًا وفقًا لأبرز منصات التقييم، حيث حققت تصنيفًا متميزًا بلغ 4.9 من 5، بناءً على أكثر من 1,000 مراجعة. تعكس هذه النتائج مكانة TECH كمرجع أكاديمي دولي، مما يعزز جودة نموذجها التعليمي وأثره الإيجابي على طلابها.

Google Partner Premier

حصلت TECH على شارة Google Partner Premier المرموقة من عملاق التكنولوجيا الأمريكي. هذا التقدير، الذي لا تحصل عليه سوى 3% من الشركات في العالم، يبرز تجربة التعلم الفعالة والمرنة والمبتكرة التي توفرها الجامعة لطلابها. ولا يقتصر هذا الاعتراف على تأكيد أعلى معايير الجودة الأكاديمية، بل يعزز مكانة TECH كإحدى أبرز المؤسسات التكنولوجية في العالم.

03

خطة الدراسة

يهدف برنامج الماجستير المتقدم في الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات) إلى تدريب القادة الاستراتيجيين القادرين على إدارة أمن المعلومات في المؤسسات العالمية. من خلال نهج شامل ومحدّث، يغطي البرنامج مجالات رئيسية مثل حوكمة الأمن السيبراني وإدارة المخاطر. بهذه الطريقة، سيطور الطلاب مهارات إدارية لقيادة فرق عالية الأداء وتنفيذ السياسات الأمنية. بالإضافة إلى ذلك، أثناء اكتساب المعرفة بأحدث الاتجاهات والتقنيات الناشئة، سيتعلم الخريجون كيفية مواجهة تحديات البيئة الرقمية وقيادة الأمن في المستقبل.

تُعدك TECH لتكون الخبير الاستراتيجي الذي يمنع التهديدات السيبرانية ويكشفها ويخفف من حدتها في بيئة الأعمال العالمية"

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 Freenetg 2IP
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. الإستراتيجية الوطنية للأمن الإلكترونى 1290
3.8.1. مجموعة من المعايير الدولية لأمن المعلومات ISO 00027
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 32027
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. المعهد الوطني للأمن الإلكترونى
4.10.1. منظمة الدول الأمريكية
5.10.1. UNASUR - PROSUR

الوحدة 2. أمان Host

1.2. نسخ احتياطية
1.1.2. استراتيجيات النسخ الاحتياطية
2.1.2. أدوات ويندوز
3.1.2. أدوات لنظام Linux
4.1.2. أدوات لنظام MacOS
2.2. برنامج مكافحة الفيروسات للمستخدم
1.2.2. أنواع مضادات الفيروسات
2.2.2. مضاد فيروسات Windows
3.2.2. مضاد فيروسات Linux
4.2.2. مضاد فيروسات لنظام MacOS
5.2.2. مضاد فيروسات للهواتف الذكية smartphones
3.2. أجهزة كشف التسلل - HIDS
1.3.2. طرق كشف التسلل
2.3.2. Sagan
3.3.2. Aide
4.3.2. Rkhunter
4.2. Firewall محلى
1.4.2. Windows لـ Firewalls
2.4.2. Linux لـ Firewalls
3.4.2. MacOS لـ Firewalls
5.2. مديرى كلمات المرور
1.5.2. Password
2.5.2. LastPass
3.5.2. KeePass
4.5.2. StickyPassword
5.5.2. RoboForm

6.2. أجهزة كشف التصيد phishing
1.6.2. الكشف اليدوي عن التصيد 1
2.6.2. أدوات antiphishing
7.2. Spyware
1.7.2. آليات التجنب
2.7.2. أدوات مكافحة برامج التجسس antispyware
8.2. أجهزة التتبع
1.8.2. تدابير لحماية النظام
2.8.2. أدوات مكافحة التعقب
9.2. EDR End Point Detection and Response
1.9.2. سلوك نظام كشف نقطة النهاية والاستجابة لها
2.9.2. الاختلافات بين كشف نقطة النهاية والاستجابة لها ومكافحة الفيروسات
3.9.2. مستقبل أنظمة كشف نقطة النهاية والاستجابة لها
10.2. السيطرة على تثبيت البرنامج
1.10.2. المستودعات ومحلات البرمجيات
2.10.2. قوائم البرامج المسموح بها أو المحظورة
3.10.2. معايير التحديث
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 نواة (نظم تشغيل) kernel لينيكس
1.3.2.3. UFW
2.3.2.3. iptables و Nftables
3.3.2.3. Firewalld
4.2.3. أنظمة الكشف على أساس سجلات النظام
1.4.2.3. أغلفة بروتوكول التحكم بالنقل TCP Wrappers
2.4.2.3. BlockHosts وdenyHosts
3.4.2.3. ban2Fai
3.3. أنظمة كشف التسلل والوقاية منه
1.3.3. الهجمات على أنظمة كشف التسلل وأنظمة الوقاية منه
2.3.3. أنظمة كشف التسلل وأنظمة الوقاية منه
1.2.3.3. نظام كشف التسلل الأكثر شعبية
2.2.3.3. موتور كشف ومنع التسلل
4.3. Firewalls جدران الحماية من الجيل القادم
1.4.3. الاختلافات بين الجيل القادم من جدران الحماية وجدار الحماية التقليدي
2.4.3. القدرات الأساسية
3.4.3. حلول الأعمال
4.4.3. جدران الحماية للخدمات cloud
1.4.4.3. سحابة Arquitectura Cloud أمازون الافتراضية الخاصة
2.4.4.3. سحابة قائمة نظام الدخول Cloud ACLs
3.4.4.3. Security Group
5.3. Proxy
1.5.3. أنواع proxy
2.5.3. استخدام proxy. المميزات والعيوب
6.3. محركات مكافحة الفيروسات
1.6.3. السياق العام للبرامج الضارة وبطاقات e
2.6.3. مشاكل محرك مكافحة الفيروسات
7.3. أنظمة حماية البريد
1.7.3. مكافحة البريد الغير مرغوب فيه Antispam
1.1.7.3. القوائم السوداء والبيضاء
2.1.7.3. مرشحات بايزي
2.7.3. (Mail Gateway (MGW

8.3. المعلومات الأمنية وإدارة الأحداث
1.8.3. المكونات والعمارة
2.8.3. قواعد الارتباط وحالات الاستخدام
3.8.3. التحديات الحالية للمعلومات الأمنية وإدارة الأحداث
9.3. التنسيق الأمني والأتمتة والاستجابة
1.9.3. SOAR و SIEM: أعداء أو حلفاء
2.9.3. مستقبل أنظمة التنسيق الأمني والأتمتة والاستجابة
10.3 ص. نظم أخرى قائمة في الشبكات
1.10.3. جدار الحماية لتطبيقات الويب
2.10.3. التحكم في الوصول إلى الشبكة
3.10.3. HoneyNets و HoneyPots
4.10.3. وسيط أمان الوصول إلى السحابة

الوحدة 4. أمن الهواتف الذكية smartphones

1.4. عالم الأجهزة النقالة
1.1.4. أنواع المنصات المحمولة
2.1.4. أجهزة los
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. سياسات الأمن
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. أذونات
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
21.6.4. فقدان أو سرقة الجهاز
31.6.4. 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. تركيب البرمجيات الخبيثة على الجهاز
3.2.8.4. المثابرة
4.2.8.4. تنفيذ payload واستخراج المعلومات
3.8.4. Hacking أجهزة iOS: الآليات والأدوات
4.8.4. Hacking أجهزة Android: الآليات والأدوات
9.4. اختبارات الاختراق
1.9.4. iOS PenTesting
2.9.4. Android pentesting
3.9.4. الأدوات
10.4. الحماية والأمن
1.10.4. اعدادات الامان
1.1.10.4. في أجهزة iOS
2.1.10.4. في أجهزة Android
2.10.4. إجراءات السلامة
3.10.4. أدوات الحماية

الوحدة 5. الأمن في إنترنت الأشياء IoT

1.5. الأجهزة
1.1.5. أنواع الأجهزة
2.1.5. هياكل قياسية
1.2.1.5. مشروع الشراكة العالمية
2.2.1.5. المنتدى العالمي لإنترنت الأشياء IoTWF
3.1.5. بروتوكولات التطبيق
4.1.5. تقنيات الاتصال
2.5. أجهزة إنترنت الأشياء. مجالات التطبيق
1.2.5. SmartHome
2.2.5. SmartCity
3.2.5. وسائل النقل
4.2.5. الأجهزة القابلة للارتداء Wearables
5.2.5. قطاع الصحة
6.2.5. إنترنت الأشياء

3.5. بروتوكولات الاتصال
1.3.5. برتوكول MQTT
2.3.5. فتح بروتوكول تحالف المحمول
3.3.5. بروتوكول إدارة أجهزة تحالف الجوال المفتوح OMA-DM
4.3.5. التقرير الفني 960
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. الغرسات
4.8.5. الروبوتات الجراحية
9.5. الاتصال
1.9.5. Wi-Fi/Gateway
2.9.5. بلوتوث
3.9.5. الاتصال المدمج
10.5. التأمين
1.10.5. الشبكات المعنية
2.10.5. مدير كلمات المرور
3.10.5. استخدام البروتوكولات المشفرة
4.10.5. نصائح الاستخدام

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 النهرب من IDSs firewall
4.4.6. Banner Grabbing
5.4.6. مخططات الشبكة

5.6. تعداد
1.5.6. تعداد نظام اسم المجال
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 2 Wi-Fi
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. توليدالبرامج الضارة malware
3.3.9.6. تجاوز حلول مكافحة الفيروسات
10.6 ص. 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. محلليين مجزئ يسار يمين

3.2.7. التحليل الدلالي
1.3.2.7. قواعد السمات
2.3.2.7. القواعد المنسوبة التي تحتوي على السمات المركبة S-atribuidas
3.3.2.7. القواعد المنسوبة التي تحتوي على السمات المركبة L-Atribuidas
3.7. هياكل بيانات المجمّع
1.3.7. المتغيرات
2.3.7. Arrays
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. الدوال
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
3.5.7.بنية الكود فى 68x
6.7. بنية أجهزة معمارية ARM
1.6.7. بنية معالج معمارية ARM
2.6.7. بنية بيانات معمارية ARM
3.6.7. بنية الكود في معمارية ARM
7.7. تحليل الشفرة الثابتة
1.7.7. المفككات
2.7.7. المفكك التفاعلي IDA
3.7.7. معيدي بناء الكود

8.7. تحليل الشفرة الديناميكية
1.8.7. تحليل السلوك
1.1.8.7. الاتصالات
2.1.8.7. المراقبة
2.8.7. مصححات كود Linux
3.8.7. مصححات كود Windows
9.7. صندوق الحماية
1.9.7. هندسة معمارية sandbox
2.9.7. التهرب من sandbox
3.9.7. تقنيات الكشف
4.9.7. تقنيات التهرب
5.9.7. التدابير المضادة
6.9.7. Sandbox الحماية في Linux
7.9.7. صندوق الحماية في ويندوز
8.9.7. Sandbox فى MacOS
9.9.7. Sandbox في Android
10.7. تحليل البرامج الضارة
1.10.7. مناهج تحاليل malware
2.10.7. تقنيات تشويش البرمجيات الخبيثة malware
1.2.10.7. التعتيم على الملفات التنفيذية
2.2.10.7. تقييد بيئات التنفيذ
3.10.7. أدوات تحليل البرمجيات الخبيثة

الوحدة 8. التطوير الآمن

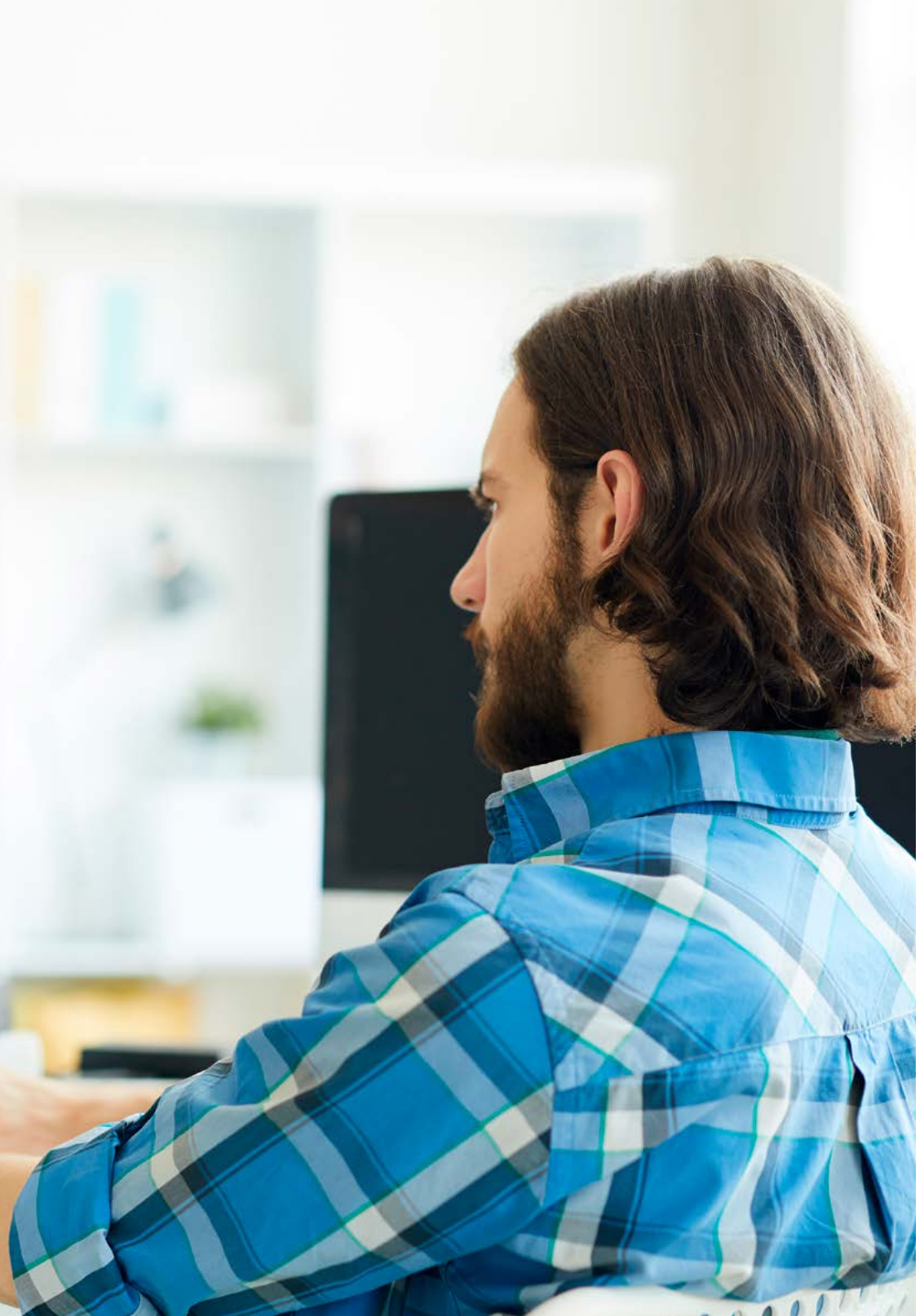
1.8. التطوير الآمن
1.1.8. الجودة والوظيفة والسلامة
2.1.8. السرية والنزاهة والتوافر
3.1.8. دورة حياة تطوير malware
2.8. مرحلة المتطلبات
1.2.8. التحكم في المصادقة
2.2.8. السيطرة على الأدوار والامتيازات
3.2.8. المتطلبات الموجهة للمخاطر
4.2.8. اعتماد الامتيازات

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. التنفيذ العملي لسياسات الأمان في البرامج والأجهزة

1.9. التنفيذ العملي لسياسات الأمان في البرامج والأجهزة
1.1.9. تنفيذ التعرف والتفويض
2.1.9. تنفيذ تقنيات التعرف
3.1.9. إجراءات التصريح التقنية
2.9. تقنيات التعرف والتفويض
1.2.9. المُعرّف ورقم التعريف الشخصي (OTP)
2.2.9. رمز USB أو بطاقة PKI الذكية
3.2.9. مفتاح "الدفاع السري"
4.2.9. تحديد الهوية بالتردد اللاسلكي النشط
3.9. السياسات الأمنية الخاصة بالوصول إلى البرامج والأنظمة
1.3.9. تنفيذ سياسات التحكم في الوصول
2.3.9. تنفيذ سياسات الوصول إلى الاتصالات
3.3.9. أنواع أدوات الأمان للتحكم في الوصول
4.9. إدارة وصول المستخدم
1.4.9. إدارة حقوق الوصول
2.4.9. الفصل بين الأدوار ووظائف الوصول
3.4.9. تطبيق حقوق الوصول في الأنظمة



5.9. التحكم في الوصول إلى الأنظمة والتطبيقات
1.5.9. قاعدة الحد الأدنى من الوصول
2.5.9. تقنيات تسجيل الدخول الآمن
3.5.9. سياسات أمان كلمات المرور
6.9. تقنيات نظام تحديد الهوية
1.6.9. الدليل النشط
2.6.9. OTP
3.6.9. PAP, CHAP
4.6.9. KERBEROS, DIAMETER, NTLM
7.9. ضوابط CIS لتأسيس النظام
1.7.9. ضوابط CIS الأساسية
2.7.9. الضوابط الرئيسية لـ CIS
3.7.9. ضوابط CIS التنظيمية
8.9. أمن العمليات
1.8.9. الحماية من الشفرات البرمجية الخبيثة
2.8.9. نسخ احتياطية
3.8.9. سجل النشاط والإشراف
9.9. إدارة الثغرات التقنية
1.9.9. نقاط الضعف التقنية
2.9.9. إدارة الثغرات التقنية
3.9.9. القيود على تثبيت software
10.9. تنفيذ ممارسات السياسة الأمنية
1.10.9. الثغرات المنطقية
2.10.9. تنفيذ السياسات الدفاعية

الوحدة 10. التحليل الجنائي

1.10. الحصول على البيانات ونسخها
1.1.10. الحصول على البيانات المتقلبة
1.1.1.10. معلومات النظام
2.1.1.10. معلومات الشبكة
3.1.1.10. ترتيب التقلب
2.1.10. الحصول على البيانات الثابتة
1.2.1.10. إنشاء صورة منسوخة
2.2.1.10. إعداد وثيقة لسلسلة الحيازة

3.1.10. طرق التحقق من صحة البيانات المكتسبة
1.3.1.10. منهجيات Linux
2.3.1.10. منهجيات Windows
2.10. تقييم وهزيمة تقنيات مكافحة الأدلة الجنائية
1.2.10. أهداف التقنيات امكافحة الأدلة الجنائية
2.2.10. مسح البيانات
1.2.2.10. حذف البيانات والملفات
2.2.2.10. استرجاع الملفات
3.2.2.10. استرجاع الأقسام المحذوفة
3.2.10. الحماية بكلمة مرور
4.2.10. إخفاء المعلومات
5.2.10. الحذف الآمن للأجهزة
6.2.10. التشفير
3.10. التحليل الجنائي لنظام التشغيل
1.3.10. التحليل الجنائي لنظام Windows
2.3.10. التحليل الجنائي لنظام Windows
3.3.10. التحليل الجنائي لنظام Mac
4.10. التحليل الجنائي للشبكة
1.4.10. تحليل السجلات
2.4.10. ترابط البيانات
3.4.10. بحث الشبكة
4.4.10. الخطوات الواجب اتباعها في التحليل الجنائي للشبكة
5.10. التحليل الجنائي للويب
1.5.10. التحقيق في هجمات الويب
2.5.10. كشف الهجمات
3.5.10. تعقب عناوين نظام منع الاختراق IPs
6.10. التحليل الجنائي لقواعد البيانات
1.6.10. التحليل الجنائي لبرنامج قواعد البيانات العلائقية MSSQL
2.6.10. التحليل الجنائي نظام إدارة قواعد البيانات MySQL
3.6.10. التحليل الجنائي في نظام إدارة قواعد البيانات PostgreSQL
4.6.10. التحليل الجنائي في نظام قاعدة بيانات مفتوحة المصدر MongoDB

7.10. التحليل الجنائي في Cloud
1.7.10. أنواع الجرائم فى Cloud
1.1.7.10. السحابة كمشتبه
2.1.7.10. السحابة كغرض
3.1.7.10. السحابة كأداة
2.7.10. تحديات التحليل الجنائى فى Cloud
3.7.10. البحث فى خدمات التخزين Cloud
4.7.10. أدوات الادلة الجنائية Cloud
8.10. التحقيق في جرائم البريد الإلكتروني
1.8.10. أنظمة البريد
1.1.8.10. عملاء البريد
2.1.8.10. خادم البريد
3.1.8.10. خادم البريد الصادر SMTP
4.1.8.10. خادم 3POP
5.1.8.10. خادم 4IMAP
2.8.10. جرائم البريد
3.8.10. رسالة بريدية
1.3.8.10. رؤوس قياسية
2.3.8.10. رؤوس ممتدة
4.8.10. خطوات التحقيق في هذه الجرائم
5.8.10. أدوات جنائية للبريد الإلكتروني
9.10. التحليل الجنائي للهواتف المحمولة
1.9.10. شبكات خلوية
1.1.9.10. أنواع الشبكات
2.1.9.10. محتويات إثبات الاستلام CDR
2.9.10. وحدة تعريف المشترك (SIM)
3.9.10. الاستحواذ المنطقي
4.9.10. الاستحواذ المادي
5.9.10. اكتساب نظام الملفات

10.10. صياغة تقارير التحليل الجنائي وتقديمها
1.10.10. الجوانب الهامة لتقرير التحليل الجنائي
2.10.10. تصنيف وأنواع التقارير
3.10.10. دليل لكتابة التقرير
4.10.10. عرض التقرير
1.4.10.10. التحضير المسبق للإدلاء بشهادة
2.4.10.10. شهادة
3.4.10.10. التعامل مع الوسائط

الوحدة 11. السلامة في التصميم وتطوير الأنظمة

1.11. نظم المعلومات
1.1.11. مجالات نظام المعلومات
2.1.11. مكونات نظام المعلومات
3.1.11. أنشطة نظام المعلومات
4.1.11. دورة حياة نظام المعلومات
5.1.11. موارد نظام المعلومات
2.11. أنظمة المعلومات الأنماط
1.2.11. أنواع نظم المعلومات
1.1.2.11. إدارة الأعمال
2.1.2.11. الاستراتيجية
3.1.2.11. حسب نطاق التطبيق
4.1.2.11. محددة
2.2.11. نظم المعلومات أمثلة حقيقية
3.2.11. تطور نظم المعلومات: المراحل
4.2.11. منهجيات نظم المعلومات
3.11. أمان نظم المعلومات. الآثار القانونية"
1.3.11. الدخول الى البيانات
2.3.11. التهديدات الأمنية نقاط الضعف
3.3.11. الآثار القانونية: الجرائم
4.3.11. إجراءات صيانة نظام المعلومات
4.11. أمان نظام المعلومات. بروتوكولات الأمن
1.4.11. أمان نظام المعلومات
1.1.4.11. نزاهة
2.1.4.11. السرية
3.1.4.11. التوفر
4.1.4.11. المصادقة
2.4.11. خدمات أمنية
3.4.11. بروتوكولات أمن المعلومات. الأنماط
4.4.11. حساسية نظام المعلومات
5.11. الأمن في نظم المعلومات. تدابير وأنظمة مراقبة الدخول
1.5.11. إجراءات السلامة
2.5.11. نوع التدابير الاحتياطية
1.2.5.11. الوقاية
2.2.5.11. الكشف
3.2.5.11. التصحيح
3.5.11. أنظمة التحكم في الدخول. الأنماط
4.5.11. علم التشفير
6.11. أمن الشبكات والإنترنت
1.6.11. جدران الحماية
2.6.11. التعريف الرقمي
3.6.11. الفيروسات والديدان
4.6.11. القرصنة Hacking
5.6.11. أمثلة وحالات حقيقية
7.11. الجريمة الإلكترونية
1.7.11. الجريمة الإلكترونية
2.7.11. الجريمة الإلكترونية الأنماط
3.7.11. الجريمة الإلكترونية الهجوم الأنماط
4.7.11. حالة الواقع الافتراضي
5.7.11. لمحات عن الجناة والضحايا. تجريم الجريمة
6.7.11. الجريمة الإلكترونية أمثلة وحالات حقيقية

8.11. الخطة الأمنية لنظام المعلومات
1.8.11. خطة الأمن الأهداف
2.8.11. خطة الأمن المخطط
3.8.11. خطة المخاطر. التحليلات
4.8.11. سياسات الأمن التنفيذ في المنظمة
5.8.11. خطة الأمن التنفيذ في المنظمة
6.8.11. الإجراءات الأمنية الأنواع
7.8.11. خطة الأمن الأمثلة
9.11. خطة الطوارئ
1.9.11. خطة الطوارئ الدوال
2.9.11. خطة الطوارئ العناصر والأهداف
3.9.11. خطة الطوارئ في المنظمة. التنفيذ
4.9.11. خطة الطوارئ الأمثلة
10.11. حوكمة أمن نظم المعلومات
1.10.11. تنظيمات قانونية
2.10.11. المعايير
3.10.11. الشهادات:
4.10.11. التقنيات

الوحدة 21. هياكل ونماذج أمن المعلومات

1.21. بنية أمن المعلومات
1.1.21. SGSI/PDS
2.1.21. التوافق الاستراتيجي
3.1.21. إدارة المخاطر
4.1.21. قياس الأداء
2.21. نماذج أمن المعلومات
1.2.21. استناداً إلى السياسات الأمنية
2.2.21. استنادًا إلى أدوات الحماية
3.2.21. قائمة على الفريق
3.21. نموذج الأمن. المكونات الرئيسية
1.3.21. تعريف المخاطر
2.3.21. تعريف الضوابط
3.3.21. التقييم المستمر لمستويات المخاطر
4.3.21. خطة التوعية للموظفين والموردين والشركاء وغيرهم
4.21. عمليات ادارة المخاطر
1.4.21. تحديد الأصول
2.4.21. الاستجابة للتهديد
3.4.21. تقييم المخاطر
4.4.21. تحديد أولويات الضوابط
5.4.21. إعادة التقييم والمخاطر المتبقية
5.21. العمليات التجارية وأمن المعلومات
1.5.21. عمليات الأعمال
2.5.21. تقييم المخاطر بناءً على معايير العمل
3.5.21. تحليل أثر الأعمال
4.5.21. العمليات التجارة وامن المعلومات
6.21. عملية التحسين المستمر
1.6.21. دورة الحياة Deming
1.1.6.21. للتخطيط
2.1.6.21. الفعل
3.1.6.21. تحقق
4.1.6.21. الفعل
7.21. معماريات الأمن
1.7.21. اختيار التقنيات وتجانسها
2.7.21. إدارة الهوية المصادقة
3.7.21. إدارة الوصول. الإذن
4.7.21. أمن البنية التحتية للشبكة
5.7.21. تقنيات وحلول التشفير
6.7.21. أمن المعدات الطرفية (EDR)
8.21. الإطار التنظيمي
1.8.21. اللوائح القطاعية
2.8.21. الشهادات:
3.8.21. التشريع
9.21. معيار ISO 10027
1.9.21. التنفيذ
2.9.21. الشهادات
3.9.21. عمليات التدقيق واختبارات الاختراق
4.9.21. إدارة المخاطر
5.9.21. تصنيف المعلومات

10.21. تشريعات الخصوصية. GDPR) RGPD)
1.10.21. نطاق اللائحة العامة لحماية البيانات (RGPD)
2.10.21. بيانات شخصية
3.10.21. الأدوار في معالجة البيانات الشخصية
4.10.21. حقوق ARCO
5.10.21. El DPO. الدوال

الوحدة 31. نظام إدارة أمن المعلومات (SGSI)

1.31. أمن المعلومات الجوانب الرئيسية
1.1.31. أمن المعلومات
1.1.1.31. السرية
2.1.1.31. نزاهة
3.1.1.31. التوفر
4.1.1.31. تدابير أمن المعلومات
2.31. نظم إدارة أمن المعلومات
1.2.31. نماذج إدارة أمن المعلومات
2.2.31. وثائق تنفيذ نظام إدارة أمن المعلومات
3.2.31. مستويات وضوابط نظام إدارة أمن المعلومات
3.31. القواعد والمعايير الدولية
1.3.31. المعايير الدولية لأمن المعلومات
2.3.31. أصل وتطور المعيار
3.3.31. معايير إدارة أمن المعلومات
4.3.31. معايير مرجعية أخرى
4.31. معيار IEC / ISO ISO 00027
1.4.31. الغرض والنطاق
2.4.31. بنية المادة
3.4.31. الشهادات
4.4.31. مراحل الاعتمادات
5.4.31. مزايا معيار IEC / ISO ISO 00027
5.31. تصميم وتنفيذ نظام أمن المعلومات الشامل
1.5.31. مراحل تنفيذ نظام أمن المعلومات الشامل
2.5.31. خطة استمرارية الأعمال

6.31. المرحلة الأولى: التشخيص
1.6.31. التشخيص الأولي
2.6.31. تحديد مستوى التقسيم الطبقي
3.6.31. مستوى الامتثال للمعايير/القواعد
7.31. المرحلة الثانية: الإعداد
1.7.31. سياق المنظمة
2.7.31. تحليل لوائح السلامة المعمول بها
3.7.31. نطاق نظام أمن المعلومات الشامل
4.7.31. سياسة نظام أمن الشامل
5.7.31. أهداف نظام أمن المعلومات الشامل
8.31. المرحلة الثالثة: التخطيط
1.8.31. تصنيف الأصول
2.8.31. تقييم المخاطر
3.8.31. تحديد التهديدات والمخاطر
9.31. المرحلة الرابعة: التنفيذ والرصد
1.9.31. تحليل النتائج
2.9.31. توزيع المسؤوليات
3.9.31. توقيت خطة العمل
4.9.31. المراقبة والتدقيق
10.31. السياسات الأمنية في إدارة الحوادث
1.10.31. المراحل
2.10.31. تصنيف الحوادث
3.10.31. إدارة الحوادث وإجراءاتها

الوحدة 14. إدارة الأمن IT

1.14. إدارة الأمن
1.1.14. العمليات الأمنية
2.1.14. الجوانب القانونية والتنظيمية
3.1.14. مؤهلات العمل
4.1.14. إدارة المخاطر
5.1.14. إدارة الهوية والوصول

2.14. هيكل المنطقة الأمنية. مكتب مدير أمن المعلومات
1.2.14. الهيكل التنظيمي موقع رئيس أمن المعلومات في الهيكلية CISO
2.2.14. خطوط الدفاع
3.2.14. المخطط التنظيمي لمكتب رئيس أمن المعلومات CISO
4.2.14. إدارة الميزانية
3.14. حكومة الأمن
1.3.14. اللجنة الأمنية
2.3.14. لجنة مراقبة المخاطر
3.3.14. لجنة التدقيق
4.3.14. لجنة الأزمات
4.14. الحكومة الأمنية. الدوال
1.4.14. السياسات والمعايير
2.4.14. خطة الأمن
3.4.14. لوحات التحكم
4.4.14. التوعية والتدريب
5.4.14. أمن سلسلة التوريد
5.14. العمليات الأمنية
1.5.14. إدارة الهوية والوصول
2.5.14. تكوين قواعد أمان الشبكة. جدران الحماية
3.5.14. إدارة منصة IDS/IPS
4.5.14. فحص الثغرات الأمنية
6.14. إطار عمل الأمن السيبراني. NIST CSF
1.6.14. منهجية NIST
1.1.6.14. تحديد
2.1.6.14. الحماية
3.1.6.14. الكشف
4.1.6.14. رد
5.1.6.14. التعافي
7.14. مركز العمليات الأمنية الدوال
1.7.14. الحماية Red Team, pentesting, threat intelligence
2.7.14. الكشف SIEM, user behavior analytics, fraud prevention
3.7.14. رد
8.14. التدقيق الأمني
1.8.14. اختبار التطفل
2.8.14. تمارين الربط الشبكي
3.8.14. تدقيق شفرة المصدر. التطوير الآمن
4.8.14. سلامة المكونات (سلسلة توريد البرمجيات)(software supply chain)
5.8.14. التحليل الجنائي
9.14. الاستجابة للحوادث
1.9.14. تحضير
2.9.14. الكشف والتحليل والإبلاغ
3.9.14. الاحتواء والاستئصال والتعافي
4.9.14. نشاط ما بعد الحادث
1.4.9.14. الاحتفاظ بالأدلة
2.4.9.14. التحليل الجنائي
3.4.9.14. إدارة الثغرات
5.9.14. الإرشادات الرسمية لإدارة الحوادث السيبرانية
10.14. إدارة الثغرات الأمنية
1.10.14. فحص الثغرات الأمنية
2.10.14. تقييم الثغرات الأمنية
3.10.14. تأسيس النظام
4.10.14. نقاط ضعف اليوم صفر. يوم الصفر

الوحدة 15. سياسات إدارة الحوادث الأمنية

1.15. سياسات إدارة حوادث أمن المعلومات وتحسيناتها
1.1.15. إدارة الحوادث
2.1.15. المسؤوليات والإجراءات
3.1.15. إشعار الحدث
2.15. أنظمة كشف التسلل والوقاية منه
1.2.15. بيانات تشغيل النظام
2.2.15. أنواع أنظمة كشف التطفل
3.2.15. معايير تحديد موقع IDS / IPS

3.15. الاستجابة للحوادث الأمنية
1.3.15. إجراءات جمع المعلومات
2.3.15. عملية التحقق من التطفل
3.3.15. هيئات فريق الاستجابة للطوارئ الحاسوبية
4.15. عملية الإخطار بمحاولة التطفل وإدارتها
1.4.15. المسؤوليات في عملية الإخطار
2.4.15. تصنيف الحوادث
3.4.15. عملية الحل والاسترداد
5.15. التحليل الجنائي كسياسة أمنية
1.5.15. الأدلة المتطايرة وغير المتطايرة
2.5.15. تحليل وجمع الأدلة الإلكترونية
1.2.5.15. تحليل الأدلة الإلكترونية
2.2.5.15. جمع الأدلة الإلكترونية
6.15. أدوات تجربة العملاء أنظمة كشف التطفل والوقاية منه (IDS/IPS)
1.6.15. نظام كشف التسلل الأكثر شعبية
2.6.15. موتور كشف ومنع التسلل
3.6.15. Solar-Winds
7.15. أدوات مركزية الحدث
1.7.15. إدارة المعلومات الأمنية (SIM)
2.7.15. التسويق عبر محركات البحث (Search Engine Marketing - SEM)
3.7.15. المعلومات الأمنية وإدارة الأحداث
8.15. دليل أمان CCN-STIC 178
1.8.15. إدارة الحوادث السيبرانية
2.8.15. المقاييس والمؤشرات
9.15. NIST / SP 16-008
1.9.15. القدرة على الاستجابة للحوادث الأمنية الحاسوبية
2.9.15. التعامل مع الحادث
3.9.15. التنسيق ومشاركة المعلومات
10.15. معايير ISO 53027
1.10.15. معايير ISO 53027. مبادئ إدارة الحوادث
2.10.15. إرشادات لتطوير خطة إدارة الحوادث
3.10.15. إرشادات عمليات الاستجابة للحوادث

الوحدة 16. تحليل المخاطر وبيئة أمن تكنولوجيا المعلومات

1.16. تحليل البيئة
1.1.16. تحليل الموقف التعليمى
1.1.1.16. بيئة VUCA
1.1.1.1.16. التقلبات
2.1.1.1.16. Incierto
3.1.1.1.16. التعقيدات
4.1.1.1.16. غامضة
2.1.1.16. بيئة BANI
1.2.1.1.16. هش
2.2.1.1.16. قلق
3.2.1.1.16. غير خطية
4.2.1.1.16. غير مفهوم
2.1.16. تحليل البيئة العامة. PESTEL
1.2.1.16. السياسي
2.2.1.16. اقتصادية
3.2.1.16. اجتماعي
4.2.1.16. التقنيات
5.2.1.16. إيكولوجي / بيئي
6.2.1.16. الشرعية
3.1.16. تحليل الوضع الداخلي. تحليل (نقاط القوة والضعف والفرص والتهديدات
1.3.1.16. الأهداف
2.3.1.16. التهديدات
3.3.1.16. الفرص
4.3.1.16. نقاط القوة
2.16. المخاطر وعدم اليقين
1.2.16. المخاطر
2.2.16. إدارة المخاطر
3.2.16. معايير إدارة المخاطر
3.16. ISO 00310: 1280 مراجعة إدارة الجودة
1.3.16. عنصر
2.3.16. الأساسيات
3.3.16. الإطار المرجعي
4.3.16. العملية

4.16. منهجية تحليل وإدارة مخاطر نظم المعلومات (MAGERIT)
1.4.16. منهجية MAGERIT
1.1.4.16. الأهداف
2.1.4.16. منهج
3.1.4.16. العناصر
4.1.4.16. التقنيات
5.1.4.16. الأدوات المتاحة (PILAR)
5.16. نقل المخاطر السيبرانية
1.5.16. نقل المخاطر
2.5.16. المخاطر السيبرانية. الأنماط
3.5.16. التأمين ضد المخاطر السيبرانية
6.16. منهجيات مرنة لإدارة المخاطر
1.6.16. المنهجيات الرشيقة
2.6.16. Scrum لإدارة المخاطر
3.6.16. AGILE Risk Management
7.16. تقنيات إدارة المخاطر
1.7.16. الذكاء الاصطناعي المطبق على إدارة المخاطر
2.7.16. Blockchain والتشفير. طرق الحفاظ على القيمة
3.7.16. الحوسبة الكمية الفرصة أو التهديد
8.16. تخطيط مخاطر تكنولوجيا المعلومات على أساس المنهجيات الرشيقة
1.8.16. تمثيل الاحتمالية والتأثير في البيئات الرشيقة
2.8.16. المخاطر كتهديد للقيمة
3.8.16. إعادة التطوير في إدارة المشاريع الرشيقة والعمليات القائمة على مؤشرات الأداء الرئيسية
9.16. Risk في إدارة المخاطر
1.9.16. Risk driven
2.9.16. Risk في إدارة المخاطر
3.9.16. تطوير نموذج لإدارة الأعمال قائم على المخاطر
10.16. الابتكار والتحول الرقمي في إدارة مخاطر تكنولوجيا المعلومات
1.10.16. الإدارة الرشيقة للمخاطر كمصدر للابتكار في الأعمال التجارية
2.10.16. تحويل البيانات إلى معلومات مفيدة في اتخاذ القرار
3.10.16. نظرة شمولية للمؤسسة من خلال المخاطر

الوحدة 17. السياسات الأمنية لتحليل تهديدات أنظمة الكمبيوتر

1.17. إدارة التهديدات في سياسات الأمان
1.1.17. إدارة المخاطر
2.1.17. المخاطر الأمنية
3.1.17. منهجيات في إدارة التهديدات
4.1.17. تطبيق المنهجيات
2.17. مراحل إدارة التهديدات
1.2.17. التعرف
2.2.17. التحليلات
3.2.17. موقع
4.2.17. تدابير الحماية
3.17. أنظمة التدقيق لتحديد موقع التهديد
1.3.17. التصنيف وتدفق المعلومات
2.3.17. تحليل العمليات الضعيفة
4.17. تصنيف المخاطر
1.4.17. أنواع المخاطر
2.4.17. حساب احتمالات التهديد
3.4.17. المخاطر المتبقية
5.17. علاج المخاطر
1.5.17. تنفيذ تدابير الحماية
2.5.17. التحويل أو الاستلام
6.17. السيطرة على المخاطر
1.6.17. العملية المستمرة لإدارة المخاطر
2.6.17. تنفيذ مقاييس الأمان
3.6.17. النموذج الاستراتيجي لمقاييس أمن المعلومات
7.17. المنهجيات العملية لتحليل التهديدات والسيطرة عليها
1.7.17. دليل التهديدات
2.7.17. دليل تدابير الرقابة
3.7.17. دليل الضمانات

8.17. معايير ISO 50027
1.8.17. تحديد المخاطر
2.8.17. تحليل المخاطر
3.8.17. تقييم المخاطر
9.17. مصفوفة المخاطر والتأثيرات والتهديدات
1.9.17. البيانات والأنظمة والموظفين
2.9.17. احتمالية التهديد
3.9.17. حجم الضرر
10.17. تصميم المراحل والعمليات في تحليل التهديدات
1.10.17. تحديد العناصر الحرجة في المنظمة
2.10.17. تحديد التهديدات والآثار
3.10.17. تحليل الأثر والمخاطر
4.10.17. المنهجيات

الوحدة 18. التنفيذ العملي للسياسات الأمنية ضد الهجمات

1.18. System Hacking
1.1.18. المخاطر ونقاط الضعف
2.1.18. التدابير المضادة
2.18. DoS في الخدمات
1.2.18. المخاطر ونقاط الضعف
2.2.18. التدابير المضادة
3.18. Session Hijacking
1.3.18. عملية Hijacking
2.3.18. التدابير المضادة لعملية Hijacking
4.18. تجاوز أنظمة IDS، الجدران النارية (Firewalls)، وفخاخ Honeypots
1.4.18. تقنيات التهرب
2.4.18. تنفيذ التدابير المضادة
5.18. Hacking Web Servers
1.5.18. الهجمات على خوادم الويب
2.5.18. تنفيذ تدابير الدفاع
6.18. Hacking Web Applications
1.6.18. الهجمات على تطبيقات الويب
2.6.18. تنفيذ تدابير الدفاع
7.18. Hacking Wireless Networks
1.7.18. نقاط الضعف في شبكات wifi
2.7.18. تنفيذ تدابير الدفاع
8.18. اختراق منصات الهواتف المحمولة
1.8.18. نقاط ضعف منصات الهواتف المحمولة
2.8.18. تنفيذ التدابير المضادة
9.18. برامج الفدية الخبيثة
1.9.18. الثغرات الأمنية المسببة لبرامج الفدية Ransomware الخبيثة
2.9.18. تنفيذ التدابير المضادة
10.18. الهندسة الاجتماعية
1.10.18. أنواع الهندسة الاجتماعية
2.10.18. التدابير المضادة للهندسة الاجتماعية

الوحدة 19. التشفير في تكنولوجيا المعلومات

1.19. علم التشفير
1.1.19. علم التشفير
2.1.19. أساسيات حسابية
2.19. علم التشفير
1.2.19. علم التشفير
2.2.19. تحليل الشفرات
3.2.19. إخفاء المعلومات وتحليل إخفاء المعلومات
3.19. بروتوكولات التشفير
1.3.19. الكتل الأساسية
2.3.19. البروتوكولات الأساسية
3.3.19. البروتوكولات الوسيطة
4.3.19. البروتوكولات المتقدمة
5.3.19. البروتوكولات الخارجية
4.19. تقنيات التشفير
1.4.19. طول المفتاح
2.4.19. الإدارة الرئيسية
3.4.19. أنواع الخوارزميات
4.4.19. ملخص الوظائف. تجزئة
5.4.19. مولدات الأرقام العشوائية الزائفة
6.4.19. استخدام الخوارزميات

الوحدة 20. إدارة الهوية والوصول في أمن تكنولوجيا المعلومات

1.20. إدارة الهوية والوصول (IAM)
1.1.20. الهوية الرقمية
2.1.20. إدارة الهوية
3.1.20. اتحاد الهويات
2.20. التحكم في الوصول المادي
1.2.20. أنظمة الحماية
2.2.20. أمن المناطق
3.2.20. مرافق الاسترداد
3.20. التحكم في الوصول المنطق
1.1.20. المصادقة الأنماط
2.1.20. بروتوكولات التوثيق
3.1.20. هجمات المصادقة
4.20. التحكم في الوصول المنطق مصادقة MFA
1.4.20. التحكم في الوصول المنطق مصادقة MFA
2.4.20. كلمة المرور: الأهمية
3.4.20. هجمات المصادقة
5.20. التحكم في الوصول المنطق المصادقة البيومترية
1.5.20. التحكم في الوصول المنطقي. المصادقة البيومترية
1.1.5.20. المصادقة البيومترية المتطلبات
2.5.20. التشغيل
3.5.20. أدوات وتقنيات
6.20. نظام إدارة الشركة
1.6.20. Single sign on
2.6.20. Kerberos
3.6.20. أنظمة AAA
7.20. أنظمة إدارة المصادقة: أنظمة AAA
1.7.20. TACACS
2.7.20. RADIUS
3.7.20. DIAMETER

5.19. التشفير المتماثل
1.5.19. شفرات التشفير المجمعة
2.5.19. DES (Data Encryption Standard)
3.5.19. خوارزمية 4RC
4.5.19. AES (Advanced Encryption Standard)
5.5.19. مزيج من شفرات الكتل
6.5.19. اشتقاق المفتاح
6.19. التشفير غير المتماثل
1.6.19. Diffie-Hellman
2.6.19. DSA (خوارزمية التوقيع الرقمي)
3.6.19. RSA (Rivest، Shamir y Adleman)
4.6.19. المنحنى البيضاوي
5.6.19. التشفير غير المتماثل الأنماط
7.19. شهادات رقمية
1.7.19. التوقيع الرقمي
2.7.19. شهادات 905X
3.7.19. البنية التحتية للمفاتيح العامة (PKI)
8.19. التنفيذ
1.8.19. Kerberos
2.8.19. IBM CCA
3.8.19. PGP (Pretty Good Privacy)
4.8.19. ISO Authentication Framework
5.8.19. SSL y TLS
6.8.19. EMV (Tarjetas inteligentes en medios de pago)
7.8.19. بروتوكولات الاتصال الهاتفي عبر الهاتف المحمول
8.8.19. Blockchain
9.19. إخفاء المعلومات
1.9.19. إخفاء المعلومات
2.9.19. تحليل التخفي
3.9.19. تطبيقات واستخدامات
10.19. التشفير الكمي
1.10.19. خوارزميات الكم
2.10.19. حماية الخوارزميات من الحوسبة الكمية
3.10.19. توزيع المفاتيح الكمية

8.20. خدمات التحكم في الوصول
1.8.20. FW-حائط الحماية من الحرائق FIREWALL
2.8.20. الشبكات الخاصة الافتراضية VPN
3.8.20. IDS- أنظمة الكشف عن التسلل
9.20. أنظمة التحكم في الوصول إلى الشبكة
1.9.20. التحكم في الوصول إلى الشبكة
2.9.20. الهندسة المعمارية والعناصر
3.9.20. التشغيل والتوحيد القياسي
10.20. دخول الشبكات اللاسلكية
1.10.20. أنواع الشبكات اللاسلكية
2.10.20. أمان الشبكة اللاسلكية
3.10.20. هجمات الشبكات اللاسلكية

الوحدة 21. الأمن في الاتصالات وتشغيل البرامج

1.21. أمن الكمبيوتر في الاتصالات وتشغيل البرامج
1.1.21. أمن تكنولوجيا المعلومات
2.1.21. الأمن السيبراني
3.1.21. أمان السحابة
2.21. أمن الكمبيوتر في الاتصالات وتشغيل البرامج. الأنماط
1.2.21. الأمن المادي
2.2.21. الأمن المنطقي
3.21. أمن الاتصالات
1.3.21. العناصر الرئيسية
2.3.21. أمن الشبكة
3.3.21. أفضل الممارسات
4.21. الذكاء السيبراني
1.4.21. الهندسة الاجتماعية
2.4.21. Deep web
3.4.21. Phishing
4.4.21. البرمجيات الخبيثة

5.21. التطوير الآمن في الاتصالات وتشغيل البرامج
1.1.21. التطوير الآمن بروتوكول HTTP
2.1.21. التطوير الآمن دورة الحياة
3.1.21. التطوير الآمن أمان PHP
4.1.21. التطوير الآمن أمان NET
5.1.21. التطوير الآمن أفضل الممارسات
6.21. أنظمة إدارة أمن معلومات الاتصالات وتشغيل البرمجيات
1.6.21. GDPR
2.6.21. CUGBP Elav-like family member 21027
3.6.21. ISO 18/17027
7.21. تكنولوجيا SIEM
1.7.21. تكنولوجيا SIEM
2.7.21. تشغيل SOC
3.7.21. SIEM موردو SIEM vendors
8.21. دور الأمن في التعبير عن الذات
1.8.21. الأدوار في المنظمات
2.8.21. دور متخصصي إنترنت الأشياءIoT في الشركات
3.8.21. الشهادات المعترف بها في السوق
9.21. التحليل الجنائي
1.9.21. التحليل الجنائي
2.9.21. التحليل الجنائي المنهجية
3.9.21. التحليل الجنائي الأدوات والتنفيذ
10.21. الأمن السيبراني اليوم
1.10.21. الهجمات الرئيسية
2.10.21. توقعات التوظيف
3.10.21. التحديات

الوحدة 22. الأمان في البيئات السحابيةCloud

1.22. الأمن في بيئات Cloud Computing
1.1.22. الأمن في بيئات Cloud Computing
2.1.22. الأمن في بيئات Cloud Computing التهديدات والمخاطر الأمنية
3.1.22. الأمن في بيئات Cloud Computing الجوانب الرئيسية للتنفيذ

2.22. أنواع البنية التحتية Cloud
1.2.22. الجمهور
2.2.22. خاص
3.2.22. هجين
3.22. نموذج الإدارة المشتركة
1.3.22. ميزات الأمن التي يديرها البائع
2.3.22. العناصر التي يديرها العميل
3.3.22. تحديد الاستراتيجية الأمنية
4.22. الآليات الوقائية
1.4.22. نظام إدارة الشركة
2.4.22. نظام إدارة الإذن: سياسات الوصول
3.4.22. أنظمة الإدارة الرئيسية
5.22. تأمين الأنظمة
1.5.22. التأمين أنظمة التخزين
2.5.22. حماية أنظمة قواعد البيانات
3.5.22. تأمين البيانات أثناء النقل
6.22. حماية البنية التحتية
1.6.22. تصميم الشبكة الآمنة وتنفيذها
2.6.22. أمن موارد الحوسبة
3.6.22. أدوات وموارد لحماية البنية التحتية
7.22. الكشف عن التهديدات والهجمات
1.7.22. أنظمة التدقيق و Logging والمراقبة
2.7.22. أنظمة الفعاليات والإنذار
3.7.22. أنظمة SIEM
8.22. الاستجابة للحوادث
1.8.22. خطة الاستجابة للحوادث
2.8.22. استمرارية الأعمال
3.8.22. تحليل الطب الشرعي ومعالجة الحوادث من نفس الطبيعة
9.22. الأمن في السحابة العامةClouds
1.9.22. AWS(خدمات أمازون على الويب)
2.9.22. Microsoft Azure
3.9.22. Google GCP
4.9.22. Oracle Cloud
10.22. اللوائح التنظيمية والامتثال
1.10.22. الامتثال للوائح السلامة
2.10.22. إدارة المخاطر
3.10.22. أشخاص الإجراءات في المنظمات

الوحدة 32. أدوات مراقبة السياسة الأمنية لنظم المعلومات

1.32. سياسات مراقبة نظم المعلومات
1.1.32. مراقبة النظم
2.1.32. المقاييس
3.1.32. أنواع المقاييس
2.32. التدقيق والتسجيل في الأنظمة
1.2.32. التدقيق والتسجيل في Windows
2.2.32. التدقيق والتسجيل في Linux
3.32. بروتوكول SNMP Simple Network Management Protocol
1.3.32. بروتوكول SNMP
2.3.32. تشغيل SNMP
3.3.32. أدوات SNMP
4.32. مراقبة الشبكة
1.4.32. مراقبة الشبكة في أنظمة التحكم
2.4.32. أدوات المراقبة لأنظمة التحكم
5.32. Nagios نظام مراقبة الشبكة
1.5.32. Nagios
2.5.32. تشغيل Nagios
3.5.32. تثبيت Nagios
6.32. Zabbix. نظام مراقبة الشبكة
1.6.32. Zabbix
2.6.32. تشغيل Zabbix
3.6.32. تثبيت Zabbix
7.32. Cacti. نظام مراقبة الشبكة
1.7.32. Cacti
2.7.32. تشغيل Cacti
3.7.32. تثبيت Cacti

8.32. Pandora. نظام مراقبة الشبكة
1.8.32. Pandora
2.8.32. تشغيل Pandora
3.8.32. تثبيت Pandora
9.32. SolarWinds. نظام مراقبة الشبكة
1.9.32. SolarWinds
2.9.32. تشغيل SolarWinds
3.9.32. تثبيت SolarWinds
10.32. اللوائح الخاصة بالمراقبة
1.10.32. ضوابط CIS بشأن التدقيق والتسجيل
2.10.32. NIST 132-008 (الولايات المتحدة)

الوحدة 24. أمن اتصالات أجهزة إنترنت الأشياء

1.24. من القياس عن بُعد إلى إنترنت الأشياءIoT
1.1.24. القياس عن بُعد
2.1.24. الاتصال من آلة إلى آلة M2M
3.1.24. إضفاء الطابع الديمقراطي على القياس عن بُعد
2.24. النموذج المرجعي
1.2.24. النموذج المرجعي
2.2.24. بنية إنترنت الأشياء المبسطةIoT
3.24. الثغرات الأمنية في إنترنت الأشياءIoT
1.3.24. أجهزة إنترنت الأشياء
2.3.24. أجهزة إنترنت الأشياء. دراسات حالة الاستخدام
3.3.24. أجهزة إنترنت الأشياء. نقاط الضعف
4.24. اتصال إنترنت الأشياء IoT
1.4.24. شبكات PAN و LAN و WAN
2.4.24. تقنيات لاسلكية غير إنترنت الأشياء IoT
3.4.24. التقنيات اللاسلكيةLPWAN
5.24. تكنولوجيا LPWAN
1.5.24. المثلث الحديدي لشبكات LPWAN
2.5.24. نطاقات التردد الحر مقابل الفرق الموسيقية المرخصة
3.5.24. خيارات تقنية LPWAN
6.24. تقنية LoRaWAN
1.6.24. تقنية LoRaWAN
2.6.24. حالات الاستخدام LoRaWAN المنظومة
3.6.24. الأمن في LoRaWAN
7.24. تقنية Sigfox
1.7.24. تقنية Sigfox
2.7.24. حالات الاستخدام Sigfox. المنظومة
3.7.24. الأمن في Sigfox
8.24. تقنية إنترنت الأشياء الخلوية IoT
1.8.24. تقنية إنترنت الأشياء الخلوية (LTE-Mg NB-IoT)
2.8.24. حالات استخدام إنترنت الأشياء الخلوي. المنظومة
3.8.24. الأمن في الخلايا إنترنت الأشياء IoT
9.24. تقنية WiSUN
1.9.24. تقنية WiSUN
2.9.24. حالات الاستخدام المنظومة
3.9.24. أمن WiSUN
10.24. تقنيات IoT الأخرى
1.10.24. تقنيات IoT الأخرى
2.10.24. حالات الاستخدام والنظام البيئي لتقنيات إنترنت الأشياء الأخرى
3.10.24. الأمن في تقنيات إنترنت الأشياء الأخرى

الوحدة 25. خطة استمرارية الأعمال المرتبطة بالأمن

1.25. خطة استمرارية الأعمال
1.1.25. خطط استمرارية الأعمال
2.1.25. خطة استمرارية الأعمال الجوانب الرئيسية
3.1.25. خطة استمرارية الأعمال لتقييم الشركة
2.25. المقاييس في خطة استمرارية الأعمال
1.2.25. (Recovery Time Objective (RTO و (Recovery Point Objective (RPO
2.2.25. الحد الأقصى للوقت المسموح به
3.2.25. الحد الأدنى لمستويات الاسترداد
4.2.25. هدف نقطة الاسترداد

3.25. مشاريع الاستمرارية. الأنماط
1.3.25. خطة استمرارية الأعمال
2.3.25. خطة استمرارية تكنولوجيا المعلومات والاتصالات (ICTCSP)
3.3.25. خطة التعافي من الكوارث (DRP)
4.25. إدارة المخاطر المرتبطة بخطة استمرارية تصريف الأعمال
1.4.25. تحليل أثر الأعمال
2.4.25. فوائد تنفيذ عن PCN
3.4.25. العقلي القائم على المخاطر
5.25. دورة حياة خطة استمرارية الأعمال
1.5.25. المرحلة 1: تحليل التنظيم
2.5.25. المرحلة 2: تحديد استراتيجية المستمر
3.5.25. المرحلة 3: الاستجابة للطوارئ
4.5.25. المرحلة 4: الاختبار والصيانة والتدقيق
6.25. مرحلة التحليل التنظيمي لخطة استمرارية تصريف الأعمال
1.6.25. تحديد العمليات التي تقع في نطاق خطة استمرارية تصريف الأعمال
2.6.25. تحديد مجالات العمل الحرجة
3.6.25. تحديد التبعيات بين المجالات والعمليات
4.6.25. تحديد أفضل التقنيات المتاحة في أفضل التقنيات المتاحة
5.6.25. الإنجازات وضع خطة
7.25. مرحلة تحديد استراتيجية الاستمرارية في خطة استمرارية تصريف الأعمال
1.7.25. الأدوار في مرحلة تحديد الاستراتيجية
2.7.25. المهام في مرحلة تحديد الاستراتيجية
3.7.25. الإنجازات
8.25. مرحلة الاستجابة للطوارئ في خطة استمرارية تصريف الأعمال
1.8.25. الأدوار في مرحلة الاستجابة
2.8.25. المهام في هذه المرحلة
3.8.25. الإنجازات
9.25. مرحلة اختبار وصيانة ومراجعة خطة استمرارية تصاميم استمرارية الأعمال
1.9.25. الأدوار في مرحلة الاختبار والصيانة والمراجعة
2.9.25. المهام في مرحلة الاختبار والصيانة والإصلاح الشامل
3.9.25. الإنجازات
10.25. معايير ISO المرتبطة بخطط استمرارية الأعمال
1.10.25. ISO 10322:1290
2.10.25. ISO 31322:2020
3.10.25. معايير ISO والمعايير الدولية الأخرى ذات الصلة

الوحدة 26. سياسة التعافي العملية من الكوارث الأمنية

1.26. خطة التعافي من الكوارث خطة التعافي من الكوارث
1.1.26. أهداف خطة التعافي من الكوارث
2.1.26. فوائد خطة التعافي من الكوارث
3.1.26. عواقب عدم وجود خطة التعافي من الكوارث وعدم تحديثها باستمرار
2.26. إرشادات حول تحديد خطة التعافي من الكوارث
1.2.26. النطاق والأهداف
2.2.26. تصميم استراتيجية التعافي
3.2.26. توزيع الأدوار والمسؤوليات
4.2.26. جرد الأجهزة softwareg والخدمات
5.2.26. تحمل وقت التعطل وفقدان البيانات
6.2.26. تحديد الأنواع المحددة من تقييمات خطة التعافي من الكوارث المطلوبة
7.2.26. تنفيذ خطة للتدريب والتوعية والتواصل
3.26. نطاق و أهداف خطة التعافي من الكوارث
1.3.26. ضمان الاستجابة
2.3.26. المكونات التكنولوجية
3.3.26. نطاق سياسة الاستمرارية
4.26. تصميم استراتيجية التعافي من الكوارث
1.4.26. إستراتيجية التعافي من الكوارث
2.4.26. الميزانية
3.4.26. الموارد البشرية والبدنية
4.4.26. المناصب الإدارية المعرضة للخطر
5.4.26. التقنيات
6.4.26. بيانات

5.26. استمرارية عمليات المعلومات
1.5.26. تخطيط الاستمرارية
2.5.26. تنفيذ الاستمرارية
3.5.26. التحقق من تقييم الاستمرارية
6.26. نطاق خطة استمرارية الأعمال
1.6.26. تحديد العمليات الأكثر أهمية
2.6.26. النهج القائم على الأصول
3.6.26. النهج القائم على العملية
7.26. تنفيذ العمليات الآمنة للأعمال التجارية
1.7.26. الأنشطة ذات الأولوية
2.7.26. أوقات التعافي المثالية
3.7.26. استراتيجيات البقاء على قيد الحياة
8.26. تحليل التنظيم
1.8.26. الحصول على المعلومات
2.8.26. تحليل الأثر على الأعمال
3.8.26. تحليل المخاطر في المنظمة
9.26. الاستجابة للطوارئ
1.9.26. خطة الأزمات
2.9.26. خطط استعادة البيئة التشغيلية
3.9.26. الإجراءات التقنية للعمل أو الحوادث
10.26. المعيار الدولي ISO 31027 ISO 31027 BCP
1.10.26. الأهداف
2.10.26. المصطلحات والتعريفات
3.10.26. عملية

الوحدة 27. تطبيق سياسات الأمن المادي والبيئي في الشركة

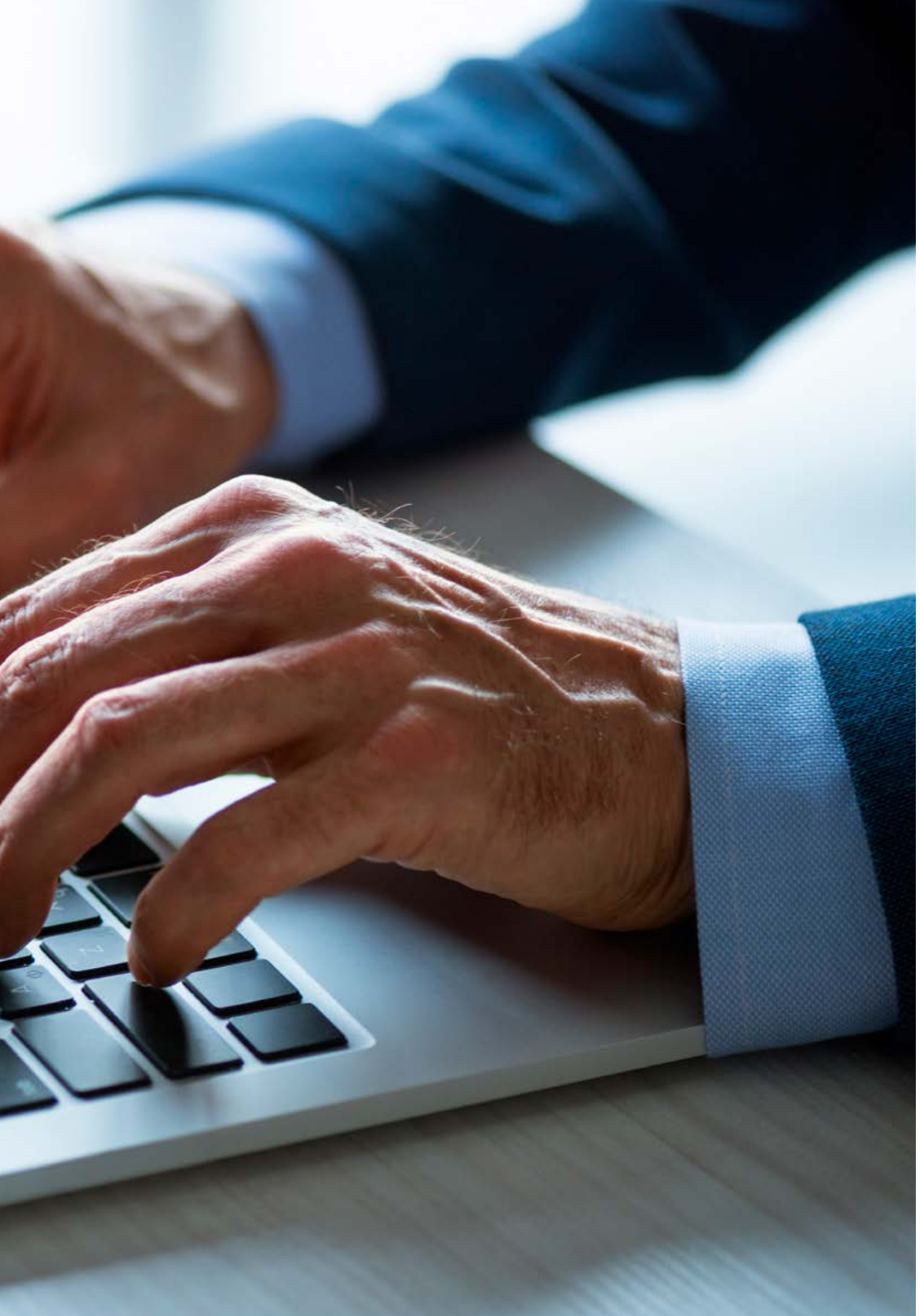
1.27. المناطق الامنة
1.1.27. المحيط الأمني المادي
2.1.27. العمل في المناطق الآمنة
3.1.27. أمن المكاتب والمرافق والموارد
2.27. الضوابط المادية للدخول
1.2.27. سياسات التحكم في الوصول المادي
2.2.27. أنظمة التحكم المادي في الدخول
3.27. نقاط ضعف الدخول المادي
1.3.27. نقاط الضعف المادية الرئيسية
2.3.27. تنفيذ تدابير الحماية
4.27. أنظمة القياسات الحيوية الفسيولوجية
1.4.27. البصمة
2.4.27. التعرف على الوجه
3.4.27. التعرف على القزحية وشبكية العين
4.4.27. أنظمة القياسات الحيوية الفسيولوجية الأخرى
5.27. الأنظمة البيومترية السلوكية
1.5.27. التعرف على التواقيع
2.5.27. التعرف على الكاتب
3.5.27. التعرف الصوتي
4.5.27. الأنظمة البيومترية السلوكية الأخرى
6.27. إدارة المخاطر في القياسات الحيوية
1.6.27. تنفيذ أنظمة القياسات الحيوية
2.6.27. نقاط الضعف في الأنظمة البيومترية
7.27. تطبيق السياسة على المضيفين
1.7.27. تركيب كابلات الإمداد والأمن
2.7.27. مواقع المعدات
3.7.27. خروج المعدات إلى خارج المبنى
4.7.27. معدات تكنولوجيا المعلومات غير المراقبة وسياسة تطهير المكاتب
8.27. حماية البيئة
1.8.27. نظام الحماية من الحرائق
2.8.27. نظام الحماية من الهزات
3.8.27. أنظمة الحماية من الزلازل
9.27. الأمن في مركز معالجة البيانات
1.9.27. أبواب الأمان
2.9.27. نظم المراقبة بالفيديو (CCTV)
3.9.27. التحكم الأمني
10.27. لوائح السلامة البدنية الدولية
1.10.27. IEC 1-2-34246 الأوربية
2.10.27. NERC CIP 5-500 (الولايات المتحدة)
3.10.27. NERC CIP 2-140 (الولايات المتحدة)

الوحدة 28. سياسات الاتصالات الآمنة في المؤسسة

1.28. إدارة أمن الشبكة
1.1.28. التحكم في الشبكة ومراقبتها
2.1.28. فصل الشبكات
3.1.28. أنظمة أمن الشبكات
2.28. بروتوكولات الاتصال الأمنة
1.2.28. نموذج TCP / IP
2.2.28. بروتوكول IPSEC
3.2.28. بروتوكول TLS
3.28. بروتوكول TLS 3.1
1.3.28. مراحل عملية 3.1TLS
2.3.28. بروتوكول المصافحة بالأيدي Handshake
3.3.28. بروتوكول التسجيل
4.3.28. الاختلافات مع TLS 2.1
4.28. خوارزميات التشفير
1.4.28. خوارزميات التشفير المستخدمة في الاتصالات
2.4.28. Cipher-suites
3.4.28. خوارزميات التشفير المسموح بها في TLS 3.1
5.28. وظائف Digest
1.5.28. 6MD
2.5.28. SHA
6.28. البنية التحتية للمفاتيح العامة PKI
1.6.28. PKI والكيانات التابعة لها
2.6.28. شهادة رقمية
3.6.28. أنواع الشهادات الرقمية
7.28. الاتصالات عبر الأنفاق والنقل
1.7.28. اتصالات الأنفاق
2.7.28. اتصالات النقل
3.7.28. تنفيذ النفق المشفر
8.28. SSH. Secure Shell
1.8.28. SSH. كبسولة آمنة
2.8.28. تشغيل SSH
3.8.28. أدوات SSH
9.28. التدقيق في أنظمة التشفير
1.9.28. اختبار السلامة
2.9.28. اختبار نظام التشفير
10.28. أنظمة التشفير
1.10.28. نقاط ضعف أنظمة التشفير
2.10.28. الضمانات في التشفير

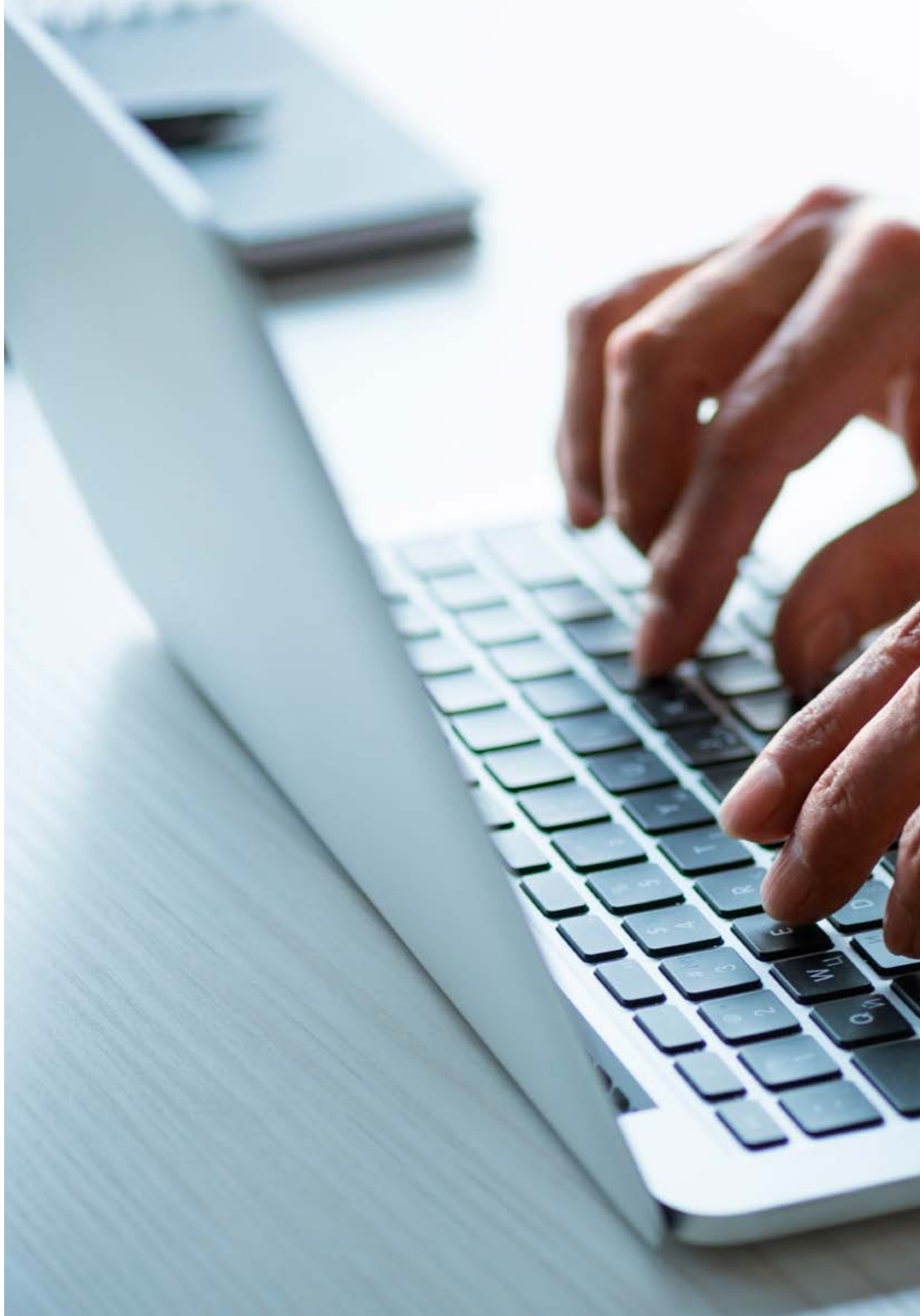
الوحدة 29. الجوانب التنظيمية لسياسة أمن المعلومات

1.29. التنظيم الداخلي
1.1.29. توزيع المسؤوليات
2.1.29. الفصل بين المهام
3.1.29. الاتصالات مع السلطات
4.1.29. أمن المعلومات في إدارة المشاريع
2.29. إدارة الأصول
1.2.29. التزامات الأصول
2.2.29. تصنيف المعلومات
3.2.29. التعامل مع وسائط التخزين
3.29. السياسات الأمنية في عمليات الأعمال
1.3.29. تحليل عمليات الأعمال المعرضة للخطر
2.3.29. تحليل أثر الأعمال
3.3.29. تصنيف العمليات فيما يتعلق بتأثيرها على الأعمال
4.29. السياسات الأمنية المرتبطة بالموارد البشرية
1.4.29. قبل التعيين
2.4.29. أثناء التعيين
3.4.29. إنهاء الخدمة أو تغيير المنصب



5.29. السياسات الأمنية في الادارة
1.5.29. إرشادات الإدارة بشأن أمن المعلومات
2.5.29. تحليل تأثير الأعمال- تحليل الأثر
3.5.29. خطة التعافي كسياسة أمنية
6.29. اقتناء وصيانة نظم المعلومات
1.6.29. متطلبات أمن نظم المعلومات
2.6.29. أمن بيانات التطوير والدعم
3.6.29. بيانات الاختبار
7.29. الأمن مع الموردين
1.7.29. أمن تكنولوجيا المعلومات مع الموردين
2.7.29. إدارة تقديم الخدمات مع ضمان تقديم الخدمات
3.7.29. أمن سلسلة التوريد
8.29. السلامة في العمليات
1.8.29. المسؤوليات في العملية
2.8.29. الحماية من الشفرات البرمجية الخبيثة
3.8.29. نسخ احتياطية
4.8.29. سجل النشاط والإشراف
9.29. الإدارة الأمنية والتنظيمية
1.9.29. الامتثال للمتطلبات القانونية
2.9.29. مراجعات في أمن المعلومات
10.29. الأمن في إدارة استمرارية الأعمال
1.10.29. الاستمرارية في أمن المعلومات
2.10.29. حالات التكرار

سيعلمك المنهج الدراسي الكامل للتكنولوجيا التقنية كيف تكون قائدًا ذا رؤية تضمن حماية المؤسسة على المدى الطويل"



04

أهداف التدريس

يهدف برنامج الماجستير المتقدم في الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات) إلى تدريب القادة الاستراتيجيين القادرين على إدارة أمن المعلومات في أي نوع من المؤسسات. سيطور المشاركون خلال البرنامج كفاءاتهم لتحديد المخاطر السيبرانية وتقييمها والتخفيف من حدتها، وتنفيذ سياسات أمنية فعالة. بالإضافة إلى ذلك، سيتم تزويدهم بفهم متعمق للتقنيات الناشئة وأفضل الممارسات في مجال البنية الأمنية، بما يضمن حماية البيانات واستمرارية الأعمال. كما يعزز البرنامج أيضاً رؤية متكاملة للأعمال في مجال الأمن السيبراني، ومواءمة المبادرات مع أهداف الشركة وضمان الامتثال للمعايير الدولية. سيتم إعداد الطلاب ليكونوا عوامل للتغيير وتعزيز ثقافة مؤسسية تركز على الحماية الرقمية.

ستجد في هذا التخصص المتاح 100% عبر الإنترنت أحدث المواد التعليمية والأبحاث على الساحة الجامعية"

الأهداف العامة

- تطوير قادة الأمن السيبراني الاستراتيجيين القادرين على إدارة حماية الأصول الرقمية والبنى التحتية التكنولوجية للمؤسسات العالمية
- دمج الأمن السيبراني في استراتيجية العمل، ومواءمة مبادرات الحماية الرقمية مع الأهداف العامة للمؤسسة
- التدريب على تنفيذ سياسات الأمن السيبراني والأطر التنظيمية التي تضمن الامتثال التنظيمي وحماية المعلومات في البيئات الرقمية
- تعزيز قيادة وإدارة فرق الأمن السيبراني وتحسين القدرة على اتخاذ القرارات الاستراتيجية في حالات الأزمات وإدارة المشاريع الأمنية على المستوى التنظيمي

> انضم إلى TECH وطوّر المهارات التي تحتاجها لتصبح قائداً يستبق التهديدات ويعزز الفرص"

الأهداف المحددة

الوحدة 1. الذكاء والأمن السيبراني

- تطوير المهارات اللازمة لتنفيذ استراتيجيات الاستخبارات الإلكترونية والأمن السيبراني
- حماية أنظمة تكنولوجيا المعلومات من التهديدات السيبرانية من خلال جمع المعلومات الرقمية وتحليلها واستخدامها

الوحدة 2. أمان Host

- التدريب على تنفيذ التدابير الأمنية في الأنظمة المضيفة
- ضمان حماية الخوادم والأجهزة من نقاط الضعف والبرامج الضارة malware والوصول غير المصرح به

الوحدة 3. أمان الشبكة (المحيط)

- توفير المعرفة اللازمة لحماية شبكات الكمبيوتر على مستوى المحيط الخارجي
- إدارة الأدوات والتقنيات الأمنية مثل جدران الحماية والشبكات الافتراضية الخاصة وأنظمة كشف التسلل

الوحدة 4. أمن الهواتف الذكية smartphones

- توفير فهم شامل لأمن الأجهزة المحمولة
- تعزيز الحماية ضد التهديدات مثل البرمجيات الخبيثة malware وفقدان البيانات والهجمات عبر تطبيقات الهاتف المحمول

الوحدة 5. الأمن في إنترنت الأشياء IoT

- التدريب على تنفيذ السياسة الأمنية لأجهزة إنترنت الأشياء
- تأمين البنية التحتية والبيانات الناتجة عن الأجهزة المتصلة من خلال الشبكات ومنصات إنترنت الأشياء

الوحدة 6. Hacking أخلاقيات

- تطوير المهارات اللازمة لإجراء اختبارات الاختراق والتدقيق الأمني باستخدام تقنيات القرصنة الأخلاقية
- القدرة على تحديد نقاط الضعف ومنع الهجمات

الوحدة 7. الهندسة العكسية
- إتقان تقنيات الهندسة العكسية لتحليل وفهم عمل البرمجيات والأجهزة hardware
- تحديد نقاط الضعف المحتملة والحلول الأمنية

الوحدة 8. التطوير الآمن
- تدريس أفضل الممارسات في تطوير البرمجيات الآمنة
- تطبيق مبادئ الأمان طوال دورة حياة التطوير لتقليل المخاطر ونقاط الضعف في التطبيقات

الوحدة 9. التنفيذ العملي لسياسات الأمان في البرامج والأجهزة
- توفير المعرفة اللازمة لتصميم وتنفيذ سياسات أمنية قوية للبرامج والأجهزة
- ضمان الحماية من التهديدات الداخلية والخارجية

الوحدة 10. التحليل الجنائي
- تطوير المهارات في تحليل الأدلة الجنائية الرقمية
- تحليل عملية جمع الأدلة الرقمية وحفظها وتحليلها في حالات الحوادث الأمنية الحاسوبية

الوحدة 11. السلامة في التصميم وتطوير الأنظمة
- معالجة دمج التدابير الأمنية من مراحل تصميم وتطوير أنظمة تكنولوجيا المعلومات
- ضمان الحماية من نقاط الضعف المحتملة منذ بداية المشروع

الوحدة 12. هياكل ونماذج أمن المعلومات
- توفير المعرفة اللازمة حول بنيات ونماذج أمن المعلومات
- تصميم وتطبيق أنظمة قوية تحمي بيانات المؤسسة ومواردها

الوحدة 13. نظام إدارة أمن المعلومات (SGSI)
- تنفيذ نظام إدارة أمن المعلومات
- حماية المعلومات التجارية بشكل فعال، وضمان الامتثال للوائح التنظيمية وأفضل الممارسات

الوحدة 14. إدارة الأمن IT
- توفير المعرفة اللازمة لإدارة أمن البنى التحتية التكنولوجية للشركة بفعالية
- تقليل المخاطر وضمان استمرارية الأعمال

الوحدة 15. سياسات إدارة الحوادث الأمنية
- التدريب على إنشاء وتنفيذ سياسات فعالة لإدارة الحوادث الأمنية وتنفيذها
- وضع بروتوكولات واضحة للكشف عن الاختراقات الأمنية وتحليلها والاستجابة لها. الاختراقات

الوحدة 16. تحليل المخاطر وبيئة أمن تكنولوجيا المعلومات
- توفير المعرفة اللازمة لإجراء تحليل المخاطر لبيئة تقنية المعلومات، وتحديد التهديدات ونقاط الضعف
- تنفيذ استراتيجيات التخفيف من المخاطر لتأمين البنية التحتية للتكنولوجيا

الوحدة 17. السياسات الأمنية لتحليل تهديدات أنظمة الكمبيوتر
- التدريب على تطوير السياسات الأمنية لتحديد وتحليلها والتخفيف من حدة التهديدات التي تتعرض لها أنظمة تكنولوجيا المعلومات. استخدام الأدوات والأساليب المناسبة لحماية الأصول الرقمية للمؤسسة

الوحدة 18. التنفيذ العملي للسياسات الأمنية ضد الهجمات
- تنفيذ سياسات أمنية فعالة ضد الهجمات المحتملة
- ضمان حماية الأنظمة والمعلومات الهامة في المؤسسة

الوحدة 19. التشفير في تكنولوجيا المعلومات
- تدريس أساسيات وتطبيقات التشفير في مجال تكنولوجيا المعلومات
- تنفيذ خوارزميات التشفير والأمان في نقل البيانات

الوحدة 20. إدارة الهوية والوصول في أمن تكنولوجيا المعلومات
- تطوير المهارات اللازمة لإدارة الهوية والوصول في أنظمة تكنولوجيا المعلومات
- وضع سياسات المصادقة والتحكم في الوصول لحماية موارد المؤسسة وبياناتها

الوحدة 21. الأمن في الاتصالات وتشغيل البرامج
- التدريب على حماية الاتصالات الرقمية وتنفيذ التدابير الأمنية في تشغيل البرمجيات
- ضمان سرية وسلامة وتوافر المعلومات

الوحدة 22. الأمان في البيئات السحابية Cloud
- تنفيذ سياسات الأمان في بيئات الحوسبة السحابية
- ضمان حماية البيانات والتطبيقات من الوصول غير المصرح به والهجمات

الوحدة 23. أدوات مراقبة السياسة الأمنية لنظم المعلومات
- التدريب على استخدام أدوات المراقبة لتقييم فعالية سياسات أمن نظم المعلومات
- تعميق الكشف المبكر عن نقاط الضعف والهجمات

الوحدة 24. أمن اتصالات أجهزة إنترنت الأشياء
- تطوير المهارات في تنفيذ تدابير أمنية لحماية الاتصالات بين أجهزة إنترنت الأشياء و الاتصالات بين أجهزة إنترنت الأشياء
- التقليل من المخاطر المرتبطة بتبادل البيانات بين الأجهزة المتصلة

الوحدة 25. خطة استمرارية الأعمال المرتبطة بالأمن
- وضع خطة استمرارية الأعمال التي تضمن حماية الأنظمة واستعادتها السريعة
- وضع بروتوكولات لتأمين البيانات الهامة في حالة وقوع حوادث أمنية

الوحدة 26. سياسة التعافي العملية من الكوارث الأمنية
- إنشاء سياسات التعافي من الكوارث
- ضمان الاستعادة السريعة للأنظمة وحماية البيانات في حالة وقوع حوادث أمنية خطيرة

الوحدة 27. تطبيق سياسات الأمن المادي والبيئي في الشركة
- التدريب على تنفيذ سياسات الأمن المادي والبيئي لحماية الموارد المادية للمؤسسة
- ضمان البيئة المناسبة للتشغيل الآمن لأنظمة التكنولوجيا

الوحدة 28. سياسات الاتصالات الآمنة في المؤسسة
- توفير المعرفة اللازمة لتطوير سياسات الاتصالات الآمنة داخل المؤسسة
- حماية شبكات وقنوات الاتصال من التجسس وتسريب المعلومات

الوحدة 29. الجوانب التنظيمية لسياسة أمن المعلومات
- توفير الأدوات اللازمة لتنفيذ السياسات المؤسسية لإدارة أمن المعلومات
- تحديد الأدوار والمسؤوليات والعمليات المناسبة لحماية أصول المعلومات

05

الآفاق المهنية

عند الانتهاء من برنامج الماجستير المتقدم في الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات)، سيكون الخريجون مؤهلين تماماً لتولي أدوار رئيسية في حماية وإدارة أمن المعلومات في مختلف المؤسسات. بالإضافة إلى ذلك، سيكونون قادرين على قيادة الاستراتيجيات الأمنية في الشركات متعددة الجنسيات، وإدارة المخاطر السيبرانية والتخفيف من حدتها. كما سيتم إعدادهم لشغل المناصب التي تتطلب مهارات لقيادة مبادرات الأمن السيبراني وضمان حماية الأصول الرقمية في أي قطاع.

مع هذا الماجستير المتقدم سوف تتخصص كمدير
قادر على توقع المخاطر وحماية المعلومات الهامة"

ملف الخريجين

سيكون خريج برنامج الماجستير المتقدم في الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات) قائداً استراتيجياً يتمتع بفهم عميق لأمن المعلومات في سياق المؤسسات العالمية. ستكون قادراً على تصميم وتنفيذ سياسات أمنية متقدمة وقيادة فرق متعددة التخصصات. كما ستتمتع بمهارات قوية في الإدارة والحوكمة، مما سيمكنك من مواجهة تحديات الأمن السيبراني في مختلف القطاعات، وضمان حماية الأصول الرقمية. ستزودك هذه الفرصة بالأدوات التي تحتاجها للبقاء على اطلاع على أحدث اتجاهات التكنولوجيا والتكيف مع المشهد الرقمي سريع التغير.

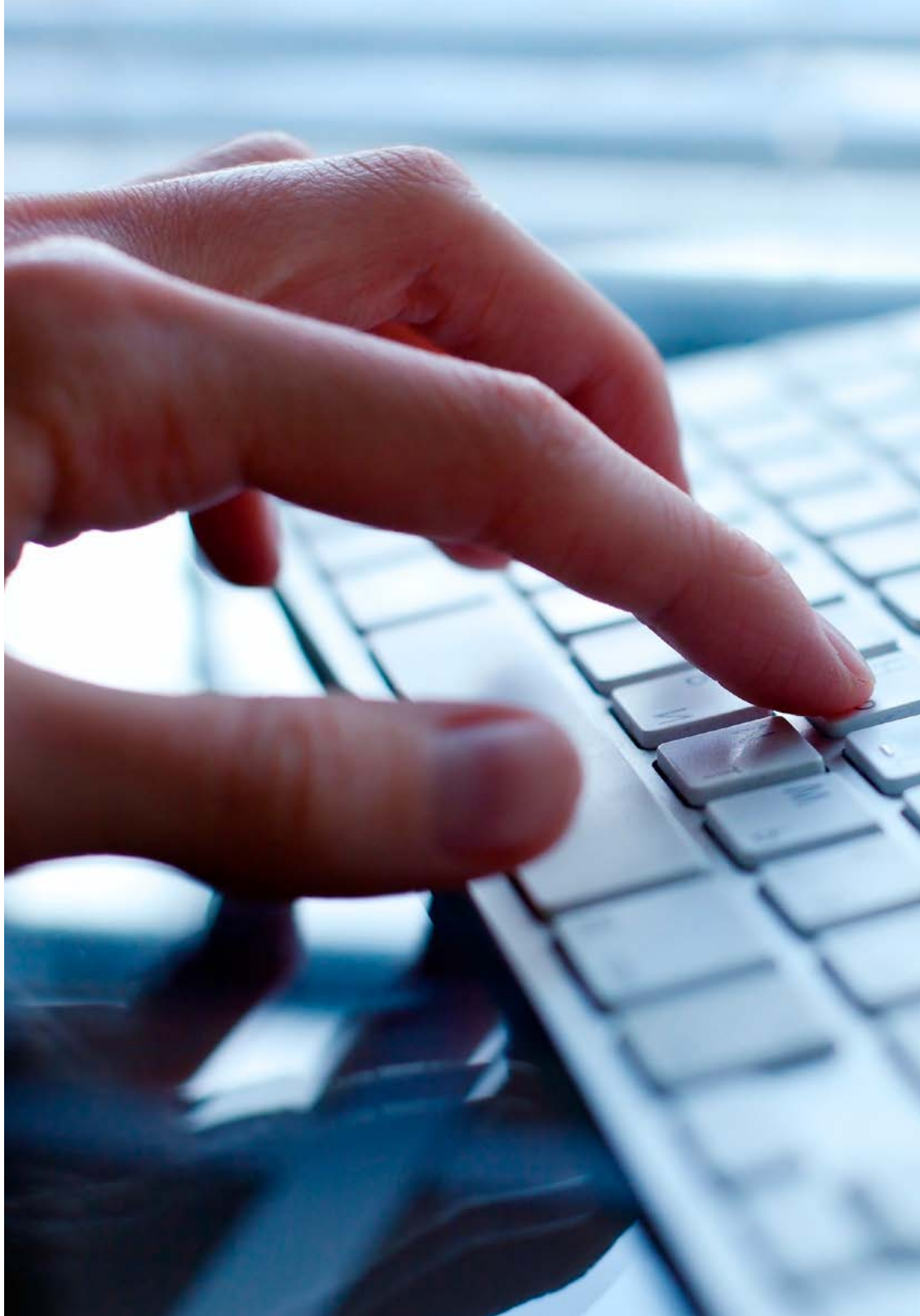
جهز نفسك لتكون من أفضل المحترفين، وقلل من تأثير الهجمات الإلكترونية وعُد إلى العمل كالمعتاد بسرعة.

- **القيادة الاستراتيجية والقدرة على التكيف:** القدرة على قيادة فرق متعددة التخصصات وإدارة السياسات الأمنية، والتكيف مع التغيرات التكنولوجية السريعة والناشئة في مجال الأمن السيبراني.
- **إدارة المخاطر واتخاذ القرارات المستنيرة:** القدرة على تحديد المخاطر السيبرانية وتقييمها والتخفيف من حدتها، واتخاذ القرارات بناءً على بيانات وتحليلات مفصلة
- **التحليل النقدي وإدارة الحوادث:** القدرة على تحديد نقاط الضعف، وإدارة الحوادث الأمنية وتنسيق الاستجابة للأزمات، وضمان استمرارية الأعمال
- **التواصل الفعال والتفكير الاستراتيجي:** القدرة على توصيل المخاطر والحلول بوضوح إلى مختلف أصحاب المصلحة، مع اتباع نهج شامل واستراتيجي لحماية الأصول الرقمية

بعد الانتهاء من الحصول على درجة الماجستير المتقدم، ستكون قادراً على استخدام معرفتك ومهاراتك في المناصب التالية:

1. **(CISO، الرئيس التنفيذي لأمن المعلومات):** قائد استراتيجي مسؤول عن حماية المعلومات والأمن السيبراني في جميع أنحاء المؤسسة، ووضع السياسات والإشراف على البنية التحتية للأمن الرقمي.
2. **مدير الأمن السيبراني:** مسؤول عن إدارة فرق أمن تكنولوجيا المعلومات والإشراف عليها، ووضع وتنفيذ استراتيجيات لحماية البنية التحتية التكنولوجية للشركة.
3. **مدير أمن تكنولوجيا المعلومات:** مسؤول عن إدارة وتنسيق سياسات الأمن الرقمي، والإشراف على حماية البيانات وأنظمة تكنولوجيا المعلومات ضد التهديدات المحتملة.
4. **مستشار الأمن السيبراني:** خبير في تقديم المشورة للشركات حول أفضل السبل لتنفيذ سياسات الأمن السيبراني وإدارتها، والمساعدة في تخفيف المخاطر والامتثال للوائح الدولية.
5. **مدير إدارة مخاطر تكنولوجيا المعلومات:** مسؤول عن تحديد وتقييم وتخفيف المخاطر السيبرانية التي قد تؤثر على أمن المعلومات والأنظمة التقنية للمؤسسة.
6. **رئيس أمن المعلومات:** القائد المسؤول عن الإشراف على جميع المبادرات المتعلقة بحماية البيانات وأنظمة تكنولوجيا المعلومات داخل المؤسسة وتنسيقها.

> أنت على بُعد خطوة واحدة من تحسين حياتك المهنية مع هذا الماجستير المتقدم الذي لا يمكن أن يقدمه سوى TECH"



06

منهجية الدراسة

TECH هي أول جامعة في العالم تجمع بين منهجيةدراسات الحالة مع التعلم المتجدد، وهو نظام تعلم 100% عبر الإنترنت قائم، قائم على التكرار الموجهتم تصميم هذه الاستراتيجية التربوية المبتكرة لتوفير الفرصة للمهنيين لتحديث معارفهم وتطوير مهاراتهم بطريقة مكثفة ودقيقة. نموذج تعلُّم يضع الطالب في مركز العملية الأكاديمية ويمنحه كل الأهمية، متكيّفًا مع احتياجاته ومتخليًا عن المناهج الأكثر تقليدية

TECH تُعدُّك لمواجهة تحديات جديدة في بيئات غير مؤكدة
وتحقيق النجاح في مسيرتك المهنية"

الطالب: الأولوية في جميع برامج TECH

في منهجية الدراسة في TECH، يعتبر الطالب البطل المطلق.

تم اختيار الأدوات التربوية لكل برنامج مع مراعاة متطلبات الوقت والتوافر والدقة الأكاديمية التي، في الوقت الحاضر، لا يطلبها الطلاب فحسب، بل أيضًا أكثر المناصب تنافسية في السوق

مع نموذج TECH التعليمي غير المتزامن، يكون الطالب هو من يختار الوقت الذي يخصصه للدراسة، وكيف يقرر تنظيم روتينه، و كل ذلك من الجهاز الإلكتروني المفضّل لديه. لن يحتاج الطالب إلى حضور دروس مباشرة، والتي غالبًا ما لا يستطيع حضورها. سيقوم بأنشطة التعلم عندما يناسبه ذلك سيستطيع دائمًا تحديد متى وأين يدرس

> في TECH لن تكون لديك دروس مباشرة (والتي لا يمكنك حضورها أبدًا لاحقًا)"

المناهج الدراسية الأكثر شمولاً على مستوى العالم

تتميز TECH بتقديم أكثر المسارات الأكاديمية اكتمالاً في المحيط الجامعي. يتم تحقيق هذه الشمولية من خلال إنشاء مناهج لا تغطي فقط المعارف الأساسية، بل تشمل أيضًا أحدث الابتكارات في كل مجال.

من خلال التحديث المستمر، تتيح هذه البرامج للطلاب البقاء على اطلاع دائم على تغييرات السوق واكتساب المهارات الأكثر قيمة لدى أصحاب العمل. وبهذه الطريقة، يحصل الذين ينهون دراساتهم في TECH الجامعة التكنولوجية على إعداد شامل يمنحهم ميزة تنافسية ملحوظة للتقدم في مساراتهم المهنية.

وبالإضافة إلى ذلك، سيتمكنون من القيام بذلك من أي جهاز، سواء كان حاسوبًا شخصيًا، أو جهازًا لوحيًا، أو هاتفًا ذكيًا.

> نموذج TECH الجامعة التكنولوجية غير متزامن، مما يسمح لك بالدراسة باستخدام حاسوبك الشخصي، أو جهازك اللوحي، أو هاتفك الذكي أينما شئت، ومتى شئت، وللمدة التي تريدها"

Case studies أو دراسات الحالة

كانت طريقة الحالة هي نظام التعلم الأكثر استخداماً من قبل أفضل الكليات في العالم. قد كان منهج الحالة النظام التعليمي الأكثر استخدامًا من قبل أفضل كليات الأعمال في العالم. تم تطويره في عام 1219 لكي لا يتعلم طلاب القانون القوانين فقط على أساس المحتوى النظري، بل كان دوره أيضًا تقديم مواقف حقيقية معقدة لهم. وهكذا، يمكنهم اتخاذ قرارات وإصدار أحكام قيمة مبنية على أسس حول كيفية حلها. في عام 1924 تم تحديد هذه المنهجية كمنهج قياسي للتدريس في جامعة Harvard.

مع هذا النموذج التعليمي، يكون الطالب نفسه هو الذي يبني كفاءته المهنية من خلال استراتيجيات مثل **التعلم بالممارسة** أو التفكير التصميمي، والتي تستخدمها مؤسسات مرموقة أخرى مثل جامعة ييل أو ستانفورد. سيتم تطبيق هذه الطريقة، الموجهة نحو العمل، طوال المسار الأكاديمي الذي سيخوضه الطالب مع TECH الجامعة التكنولوجية.

سيتم تطبيق هذه الطريقة الموجهة نحو العمل على طول المسار الأكاديمي الكامل الذي سيخوضه الطالب مع TECH. وبهذه الطريقة سيواجه مواقف حقيقية متعددة، وعليه دمج المعارف والبحث والمجادلة والدفاع عن أفكاره وقراراته. كل ذلك مع فرضية الإجابة على التساؤل حول كيفية تصرفه عند مواجهته لأحداث معقدة محددة في عمله اليومي.

طريقة Relearning

في TECH، يتم تعزيز دراسات الحالة بأفضل طريقة تدريس عبر الإنترنت بنسبة 100%: **إعادة** التعلم.

هذه الطريقة تكسر الأساليب التقليدية للتدريس لوضع الطالب في مركز المعادلة، وتزويده بأفضل المحتويات في صيغ مختلفة. بهذه الطريقة، يتمكن من مراجعة وتكرار المفاهيم الأساسية لكل مادة وتعلم كيفية تطبيقها في بيئة حقيقية.

وفي هذا السياق، وبناءً على العديد من الأبحاث العلمية، يعتبر التكرار أفضل وسيلة للتعلم. لهذا السبب، تقدم TECH بين 8 و16 تكرارًا لكل مفهوم أساسي داخل نفس الدرس، مقدمة بطرق مختلفة، بهدف ضمان ترسيخ المعرفة تمامًا خلال عملية الدراسة.

ستتيح لك منهجية إعادة التعلم والمعروفة باسم 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.

حرم جامعي افتراضي 100% عبر الإنترنت مع أفضل الموارد التعليمية.

من أجل تطبيق منهجيته بفعالية، يركز برنامج TECH على تزويد الخريجين بمواد تعليمية بأشكال مختلفة: نصوص، وفيديوهات تفاعلية، ورسوم توضيحية وخرائط معرفية وغيرها.
تم تصميمها جميعًا من قبل مدرسين مؤهلين يركزون في عملهم على الجمع بين الحالات الحقيقية وحل المواقف المعقدة من خلال المحاكاة، ودراسة السياقات المطبقة على كل مهنة مهنية والتعلم القائم على التّكرار من خلال الصوتيات والعروض التقديمية والرسوم المتحركة والصور وغيرها.

تشير أحدث الأدلة العلمية في مجال علم الأعصاب إلى أهمية مراعاة المكان والسياق الذي يتم فيه الوصول إلى المحتوى قبل البدء في عملية تعلم جديدة.
إن القدرة على ضبط هذه المتغيرات بطريقة مخصصة تساعد الأشخاص على تذكر المعرفة وتخزينها في الحُصين من أجل الاحتفاظ بها على المدى الطويل.
هذا هو نموذج يسمى التعلم الإلكتروني المعتمد على السياق العصبي المعرفي العصبي، والذي يتم تطبيقه بوعي في هذه الدرجة الجامعية.

من ناحية أخرى، ومن أجل تفضيل الاتصال بين المرشد والمتدرب قدر الإمكان، يتم توفير مجموعة واسعة من إمكانيات الاتصال، سواء في الوقت الحقيقي أو المؤجل (الرسائل الداخلية، ومنتديات المناقشة، وخدمة الهاتف، والاتصال عبر البريد الإلكتروني مع مكتب السكرتير الفني، والدردشة ومؤتمرات الفيديو)

وبالمثل، سيسمح هذا الحرم الجامعي الافتراضي المتكامل للغاية لطلاب TECH بتنظيم جداولهم الدراسية وفقًا لتوافرهم الشخصي أو التزامات العمل.
وبهذه الطريقة، سيتمكنون من التحكم الشامل في المحتويات الأكاديمية وأدواتهم التعليمية، وفقًا لتحديثهم المهني المتسارع.

> ستسمح لك طريقة الدراسة عبر الإنترنت لهذا البرنامج بتنظيم وقتك ووتيرة تعلمك، وتكييفها مع جدولك الزمني"

تُبرر فعالية المنهج بأربعة إنجازات أساسية:

1. الطلاب الذين يتبعون هذا المنهج لا يحققون فقط استيعاب المفاهيم، ولكن أيضاً تنمية قدراتهم العقلية من خلال التمارين التي تقيم المواقف الحقيقية وتقوم بتطبيق المعرفة المكتسبة.
2. يركزمنهج التعلم بقوة على المهارات العملية التي تسمح للطالب بالاندماج بشكل أفضل في العالم الحقيقي.
3. يتم تحقيق استيعاب أبسط وأكثر كفاءة للأفكار والمفاهيم، وذلك بفضل منهج المواقف التي نشأت من الواقع.
4. يصبح الشعور بكفاءة الجهد المستثمر حافزًا مهمًا للغاية للطلاب، مما يترجم إلى اهتمام أكبر بالتعلم وزيادة في الوقت المخصص للعمل في المحاضرة الجامعية.

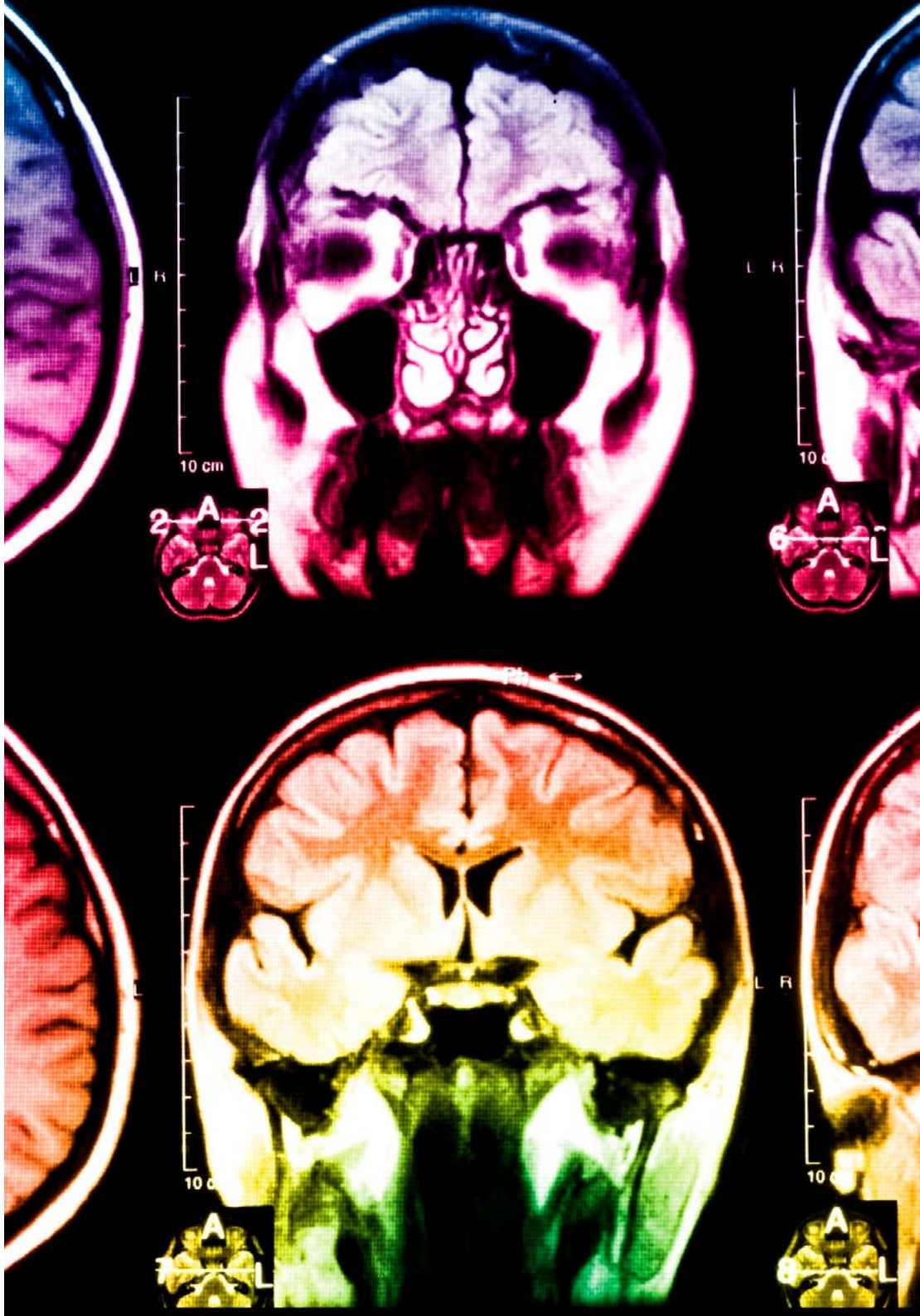
المنهجية الجامعية الأفضل تصنيفاً من قبل طلابها

نتائج هذا النموذج الأكاديمي المبتكريمكن ملاحضته في مستويات الرضا العام لخريجي TECH.

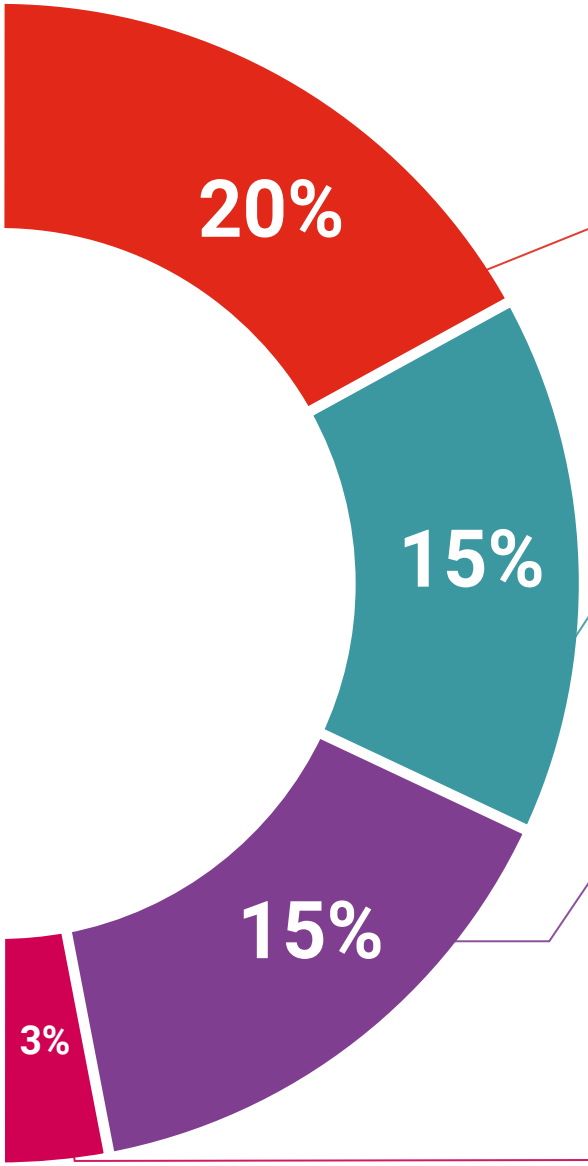
تقييم الطلاب لجودة التدريس، جودة المواد، هيكل الدورة وأهدافها ممتاز. وليس من قبيل الصدفة أن تصبح المؤسسة الجامعة الأعلى تقييماً من قبل طلابها وفقاً لمؤشر global score، حيث حصلت على 4.9 من 5.

يمكنك الوصول إلى محتويات الدراسة من أي جهاز متصل بالإنترنت (كمبيوتر، جهاز لوحي، هاتف ذكي) بفضل كون TECH على اطلاع بأحدث التطورات التكنولوجية والتربوية.

"التعلم من خبير"ستتمكن من التعلم مع مزايا الوصول إلى بيئات تعليمية محاكاة ونهج التعلم بالملاحظة، أي "التعلم من خبير"



وهكذا، ستكون أفضل المواد التعليمية، المُعدّة بعناية فائقة، متاحة في هذا البرنامج:



المواد الدراسية

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

يتم بعد ذلك تطبيق هذه المحتويات على التنسيق السمعي البصري الذي سيخلق طريقتنا في العمل عبر الإنترنت، مع التقنيات الأكثر ابتكارًا التي تتيح لنا أن نقدم لك جودة عالية، في كل قطعة سنضعها في خدمتك.

التدريب العملي على المهارات والكفاءات

ستنفذ أنشطة لتطوير كفاءات ومهارات محددة في كل مجال من مجالات المواد الدراسية. التدريب العملي والديناميكيات لاكتساب وتطوير المهارات والقدرات التي يحتاجها المتخصص لنموه في إطار العولمة التي نعيشها.

ملخصات تفاعلية

نقدم 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 من نوعه لتقديم محتوى الوسائط المتعددة على أنه"قصة نجاح أوروبية".

قراءات تكميلية

المقالات الحديثة والوثائق التوافقية والمبادئ التوجيهية الدولية... في مكتبة TECH الافتراضية، سيكون لديك وصول إلى كل ما تحتاجه لإكمال تدريبك.

دراسات الحالة (Case studies)

ستكمل مجموعة مختارة من أفضل دراسات الحالة في المادة التي يتم توظيفها.
حالات تم عرضها وتحليلها وتدريسها من قبل أفضل المتخصصين على الساحة الدولية.

الاختبار وإعادة الاختبار

نقوم بتقييم وإعادة تقييم معرفتك بشكل دوري طوال فترة البرنامج. نقوم بذلك على 3 من 4 مستويات من هرم ميلر.

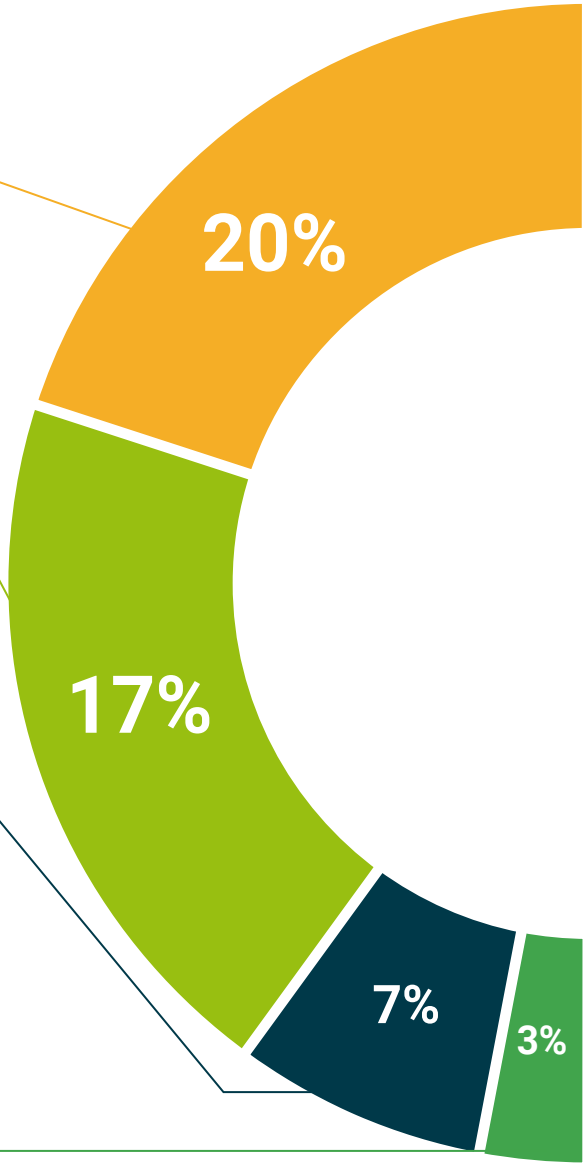
المحاضرات الرئيسية

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

إن ما يسمى **التعلم من خبير** يقوي المعرفة والذاكرة ، ويولد الأمان في قراراتنا الصعبة في المستقبل.

إرشادات توجيهية سريعة للعمل

تقدم TECH المحتويات الأكثر صلة بالدورة التدريبية في شكل أوراق عمل أو إرشادات توجيهية سريعة للعمل. إنها طريقة موجزة وعملية وفعالة لمساعدة الطلاب على التقدم في تعلمهم.



07

أعضاء هيئة التدريس

يحتوي هذا الماجستير المتقدم في الإدارة العليا للأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات) على هيئة تدريس مكونة من محترفين نشطين يعرفون الوضع الحالي لهذا المجال بإتقان، وبالتالي سينقلون جميع مفاتيح الأمن السيبراني الحالي إلى الطالب. وبهذه الطريقة، يضمن لطالب هذا البرنامج الحصول على أحدث التطورات في هذا المجال، حيث يمكنه الوصول إليها بفضل هيئة التدريس المرموقة التي اختارتها TECH.

تقدم لك TECH المديرين والمعلمين الأكثر تخصصًا حتى يكون نهجك وتعلمك هو الأفضل"

المدير الدولي المستضاف

الدكتور Frederic Lemieux معروف عالميًا كخبير مبتكر وقائد ملهم في مجالات **الاستخبارات والأمن القومي والأمن الداخلي والأمن السيبراني والتقنيات الثورية.** 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 الإلكترونى من خلال نشر العديد من المقالات في المجلات الأكاديمية، التي تتناول مكافحة الجريمة أثناء الكوارث الكبرى ومكافحة الإرهاب ووكالات الاستخبارات، والتعاون مع الشرطة. بالإضافة إلى ذلك، كان عضوًا في اللجنة ومتحدثًا رئيسيًا في العديد من المؤتمرات الوطنية والدولية، مما جعله مرجعًا في المجال الأكاديمي والمهني.

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

د. Lemieux, Frederic

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

بفضل TECH ستتمكن من التعلم
مع أفضل المحترفين في العالم"

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 DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

أ. Olalla Bonal, Martín

- مدير أول ممارسات Blockchain في EY
- أخصائي تقني 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

أ. Marcos Sbarbaro, Victoria Alicia

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

أ. Entrenas, 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

أ. Catalá Barba, José Francisco

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

أ. Peralta Alonso, Jon

- مستشار أول لحماية البيانات والأمن السيبراني في Altia
- محامي ومستشار قانوني في Arriaga Asociados مؤسسة ذات مسؤلية محدودة للاستشارات القانونية والاقتصادية.
- المستشار القانوني / المتدرب في شركة مهنية: Óscar Padura
- إجازة في القانون من جامعة Pública del País Vasco
- ماجستير في حماية البيانات من مدرسة نظام المعلومات التنفيذي Innovative School
- ماجستير في القانون من جامعة Pública del País Vasco
- ماجستير في ممارسة الإجراءات المدنية من جامعة Isabel 1 الدولية في Castilla
- مدرس في درجة الماجستير في حماية البيانات الشخصية والأمن السيبراني وقانون تكنولوجيا المعلومات والاتصالات

أ. Gonzalo Alonso, Félix

- المدير العام والمؤسس لشركة Smart REM Solutions
- رئيس قسم هندسة المخاطر والابتكار في شركة Dynargy
- المدير الإداري والشريك المؤسس لشركة الاستشارات التكنولوجية Risknova
- ماجستير في إدارة التأمين من معهد التعاون بين شركات التأمين
- شهادة في الهندسة الصناعية التقنية، تخصص إلكترونيات صناعية، جامعة Comillas البابوية.

أ. Jiménez Ramos, Álvaro

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

أ. Redondo, Jesús Serrano

- مطور ويب وفني الأمن السيبراني
- مطور ويب في Roams،Palencia
- مطور FrontEnd في تليفونيكا، مدريد
- مطور FrontEnd في أفضل شركة استشارات احترافية Best Pro Consulting، مدريد
- مُركِّب معدات وخدمات الاتصالات في Grupo Zener، Castilla،León
- 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

أ. Nogales Ávila, Javier

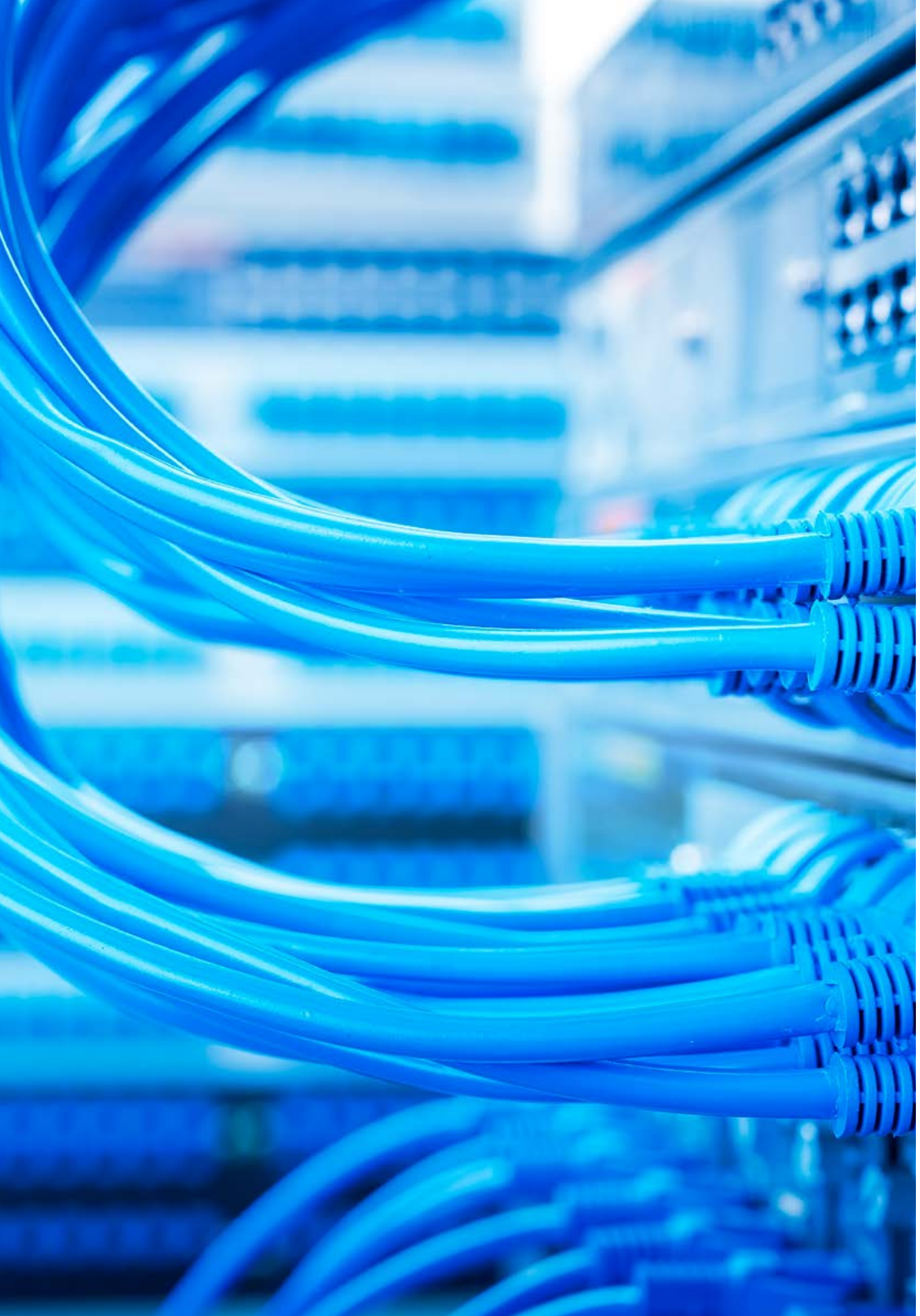
- Quint في Enterprise Cloud y Sourcing Senior Consultant
- Indra في Cloud y Technology Consultant
- Accenture في Associate Technology Consultant
- خريج هندسة المؤسسات الصناعية من جامعة Jaén
- MBA في إدارة وتسيير الشركات من كلية في ThePower Business Schooll

أ. Gómez Rodríguez, Antonio

- مهندس الحلول السحابية الرئيسي لشركة أوراكل Oracle
- منظم مشارك في ملتقى مطوري ملقة للمطورين
- مستشار متخصص في مجموعة Sopra Group y Everis
- 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

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



أ. del Valle Arias, Jorge

- مهندس اتصالات مع خبرة في تطوير الأعمال التجارية
- Smart City Solutions & Software Business Development Manager España. Itron, Inc
- مستشار انترنت الأشياء
- 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 فيSantander 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

أ. 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
- مهندس تقني في إدارة الكمبيوتر من جامعة البوليتيكنيك في مدريد.
- Certified Data Privacy Solutions Engineer (CDPSE) por ISACA

أ. Ortega Esteban, Octavio

- أخصائي التسويق وتطوير الويب
- مبرمج تطبيقات مستقل ومطور ويب مستقلFreelance
- Chief Operating Officer 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 الدراسات الجامعيه Villanueva

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

08

المؤهل العلمي

يضمن الماجستير المتقدم في الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات) بالإضافة إلى التدريب الأكثر دقة وحداثة، الحصول على مؤهل الماجستير المتقدم الصادر عن TECH الجامعة التكنولوجية.

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

تحتوي درجة **الماجستير المتقدم في الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات)** على البرنامج الأكثر اكتمالا وحداثة في السوق.

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

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

المؤهل العلمي: **ماجستير متقدم في الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات)**

طريقة الدراسة: **عبر الإنترنت**

مدة الدراسة: **2 سنتين**


tech الجامعة التكنولوجية

شهادة تخرج

هذه الشهادة ممنوحة إلى

لـ

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

لاجتيازه/لاجتيازها بنجاح والحصول على برنامج

ماجستير متقدم

في

الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات)

وهي شهادة خاصة من هذه الجامعة موافقة لـ 3000
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


الرئيس التنفيذي لأمن المعلومات) ماجستير متقدم في ،CISO) الإدارة العليا في الأمن السيبراني

التوزيع العام للخطة الدراسية

الدورة	المادة	الطريقة	عدد الساعات
1°	الذكاء والأمن السيبراني	إجباري	100
1°	أمان Host	إجباري	100
1°	أمان الشبكة (المحيط)	إجباري	100
1°	أمن الهواتف الذكية smartphones	إجباري	100
1°	الأمن في إنترنت الأشياء IoT	إجباري	100
1°	Hacking أخلاقيات	إجباري	100
1°	الهندسة العكسية	إجباري	100
1°	التطوير الآمن	إجباري	100
1°	التقييد العملي لسياسات الأمان في البرامج والأجهزة	إجباري	100
1°	التحليل الجنائي	إجباري	100
1°	السلامة في التصميم وتطوير الأنظمة	إجباري	100
1°	هياكل ونماذج أمن المعلومات	إجباري	100
1°	نظام إدارة أمن المعلومات (SGSI)	إجباري	100
1°	إدارة الأمن IT	إجباري	100
1°	سياسات إدارة الحوادث الأمنية	إجباري	100

الدورة	المادة	الطريقة	عدد الساعات
2°	تحليل المخاطر وبيئة أمن تكنولوجيا المعلومات	إجباري	100
2°	السياسات الأمنية لتحليل تهديدات أنظمة الكمبيوتر	إجباري	100
2°	التقييد العملي للسياسات الأمنية ضد الهجمات	إجباري	100
2°	التشفير في تكنولوجيا المعلومات	إجباري	100
2°	إدارة الهوية والوصول في أمن تكنولوجيا المعلومات	إجباري	100
2°	الأمن في الاتصالات وتشغيل البرامج	إجباري	100
2°	الأمان في البيانات السحابية Cloud	إجباري	100
2°	أدوات مراقبة السياسة الأمنية لنظم المعلومات	إجباري	100
2°	أمن الاتصالات لأجهزة إنترنت الأشياء	إجباري	100
2°	خطة استمرارية الأعمال المرتبطة بالأمن	إجباري	125
2°	سياسة التعافي العملية من الكوارث الأمنية	إجباري	125
2°	تطبيق سياسات الأمن المادي والبيئي في الشركة	إجباري	125
2°	سياسات الاتصالات الآمنة في المؤسسة	إجباري	125
2°	الجوانب التنظيمية لسياسة أمن المعلومات	إجباري	125

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

ماجستير متقدم
الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات)

- طريقة الدراسة: **عبر الإنترنت**
- مدة الدراسة: **2 سنتين**
- المؤهل العلمي من: **TECH الجامعة التكنولوجية**
- مواعيد الدراسة: **وفقًا لوتيرتك الخاصّة**
- الامتحانات: **عبر الإنترنت**

ماجستير متقدم

الإدارة العليا في الأمن السيبراني (CISO، الرئيس التنفيذي لأمن المعلومات)

tech الجامعة التيكنولوجية