الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التكوين والتعليم المهنيين
People's Democratic Republic of Algeria
Ministry of Vocational Training and Education

معهد التكوين والتعليم المهنيين -عنابة-

INSTITUTE OF VOCATIONAL TRAINING AND PROFESSIONAL EDUCATION

- ANNABA –

الدليل التقني والبيداغوجي للمتربص

إعلام آلي - الرقمنة - الاتصالات

أنظمة وشبكة المعلوماتية: خيار: الأمن السيبراني

المقياس

معايير وقواعد الأمن السيبراني

المستوى

٧

2026

الفهرس

التمهيد

في ظل التحول الرقمي المتسارع الذي يشهده العالم اليوم، لم يعد الاعتماد على التكنولوجيا خياراً، بل أصبح ضرورة حتمية لضمان استمرارية الأعمال. ومع هذا الاعتماد المتزايد، برزت تحديات جديدة تتمثل في التهديدات الرقمية والهجمات الخبيثة التي تستهدف البنى التحتية للمعلومات. وهنا يبرز دورك كمتخصص مستقبلي في حماية هذه الأنظمة.

فالأمن السيبراني هو مجموعة من الممارسات، والتقنيات، والعمليات المصممة لحماية الأنظمة، والشبكات، والبرامج، والبيانات من الوصول غير المصرح به، أو التخريب، أو التعديل، أو الاستغلال. لا يقتصر الأمن السيبراني على الجانب التقني البحت، بل يمتد ليشمل السياسات الإدارية، وتوعية العنصر البشري، والامتثال للمعايير الدولية لضمان تكامل وسرية وتوافر المعلومات.

وتُعتبر المعلومات في العصر الحالي الأصول الأغلى لأي مؤسسة. وتكمن الأهمية القصوى لتطبيق معايير الأمن السيبراني في النقاط التالية:

- حماية البيانات الحساسة: تأمين السجلات المالية، والبيانات الشخصية للعملاء، والملكيات الفكرية من التسريب أو السرقة.
- الوقاية من الخسائر المالية: الحد من التكاليف الباهظة التي قد تنجر عن الهجمات الرقمية، سواء كانت سرقة مباشرة، أو برمجيات فدية، أو غرامات قانونية.
- الامتثال القانوني والتنظيمي: التوافق مع القوانين والمعايير المحلية والدولية لحماية خصوصية البيانات.
- حماية السمعة المؤسسية: الحفاظ على صورة المؤسسة ومكانتها في السوق من التشويه الذي يرافق حوادث اختراق البيانات.

إن تطبيق القواعد والمعايير الأمنية ليس مجرد خطوة دفاعية، بل هو استثمار استراتيجي يضمن استقرار المؤسسة وازدهارها من خلال:

- فهم أساسيات الأمن السيبراني ومفاهيمه
- تحديد المعايير والأطر التنظيمية للأمن السيبراني
- معايير الأمن التقني والاستجابة للحوادث السيبرانية
- تدقيق الأمن السيبراني والامتثال للمعايير والتوجهات المستقبلية

وفي ظل كل هاته التحديثات فإن فهم الأمن السيبراني واحد من أهم الركائز التكنولوجية في العصر الحديث، والذي صُمم خصيصاً لاستيعاب الأسس والمبادئ التي تُبنى عليها الحماية الرقمية في بيئات العمل المعقدة والتي تعد العنصر الفعّال في حماية الأنظمة والشبكات المعلوماتية من أي اختراق قد يهدد كيان واستقرار المؤسسات.

تقديم المهنة

أنظمة وشبكة المعلوماتية: خيار: الأمن السيبراني

رمز التخصص:	INT2401
نمط التكوين:	حضوري / تمهين
المستوى المطلوب:	الثالثة ثانوي
مستوى التأهيل:	05
مدة التكوين:	30 شهرا
الشهادة:	شهادة تقني سامي((BTS

التعريف بالتخصص:

التقني سامي في الأمن السيبراني هو مهني مختص في أمن المعلومات، تتمثل مهمته في حماية الأنظمة، الأجهزة، الشبكات والبيانات الرقمية من الهجمات السيبرانية والتهديدات.

النشاطات الأساسية:

- تأمين بيانات الشركة
- تأمين الخوادم السحابية والمواقع الإلكترونية.
- كشف الثغرات الأمنية في الأنظمة
- التنبؤ بمحاولات الاختراق
- منع المتسللين أو القراصنة الإلكترونيين من التسلل.

مجالات العمل بعد التخرج:

- المؤسسات العمومية والاقتصادية
- شركات صناعية
- شركات استشارات
- شركات خدمات في الهندسة المعلوماتية (SSII)
- شركات تجارية

البطاقة 01

تقديم الوحدة

عنـوان الـــــوحدة معايير وقواعد الأمن السيبراني
رمـــز الـــــوحدة INT2401Q2
مـــدة الـــــوحدة 51 ساعـــة

هـدف الـوحـدة

(Objectif modulaire)

السلوك المرتقب (attendu Comportement)

في نهاية هذه الوحدة ،يجب أن يكون المتربص قادراً على تحديد معايير و قواعد الأمن السيبراني

الشروط العامة للتقييم (Conditions générales d'évaluation)

انـــــــطلاقا من:

- دفتر الشروط.
- تعليمات الأمن.
- التوجيهات.
- المعايير التنظيمية.

بواسطـــــــــة:

- معدات وتجهيزات الأمن (مثل: أنظمة كشف ومنع التسلل IDS/IPS، جدار الحماية ASA، أنظمة إدارة المعلومات والأحداث الأمنية....
- حلول المراقبة المناسبة.
- أدوات مراقبة أمن الشبكات (NSM)
- بيئة آلة افتراضية (Virtual Machine) مزودة بنظام (Security Onion)

المعايير العامة للأداء (Critères généraux de performance)

- ✓ التحديد الدقيق لمعايير ومقاييس إدارة الأمن.
- ✓ التحديد الدقيق للخطر المعلوماتي.
- ✓ التحديد المناسب للطرائق والمقاربات المختلفة المستخدمة.
- ✓ الإنجاز المتقن لتحليل المخاطر.
- ✓ التطبيق الدقيق لإدارة خطط العمل.
- ✓ التحليل الفعّال للتنبيهات المتعلقة بالتسللات (أو الاختراقات) المسجلة.
- ✓ الإدارة الفعّالة للحوادث.
- ✓ احترام دفتر الشروط.
- ✓ الاستغلال الصحيح والسليم لأدوات الإدارة.
- ✓ احترام منهجية (أو طريقة) العمل الموصى بها.

البطاقة 2

الأهداف الوسيطية Objectifs intermédiaires	المعايير الخاصة للأداء Critères particuliers de performance	عناصر المحتوى Éléments de contenu
أساسيات الأمن السيبراني ومفاهيمه	مفهوم الأمن السيبراني وأهميته	تحديد مفهوم الأمن السيبراني وأهم التهديدات الشائعة: • مفهوم الأمن السيبراني وأهميته • التهديدات السيبرانية الشائعة وأنواعها • مبادئ الأمن السيبراني الأساسية
المعايير والأطر التنظيمية للأمن السيبراني	المعايير الدولية والأطر التنظيمية للأمن السيبراني	تحديد المعايير الدولية للأمن السيبراني: • معايير أمن الشبكات والاتصالات • معيار :ISO/IEC 27001النظام إدارة أمن المعلومات ISMS • إطار NIST للأمن السيبراني NIST Cybersecurity Framework
	الإطار القانوني والتنظيمي الجزائري للأمن السيبراني	تحديد الأطر القانونية الجزائرية للأمن السيبراني: • الإطار القانوني والتنظيمي للأمن السيبراني في الجزائر • دور الوكالة الوطنية لأمن الأنظمة المعلوماتية ANSI • التوجيهات الوطنية لحماية البيانات الشخصية
معايير الأمن التقني والاستجابة للحوادث السيبرانية	معايير الأمن التقني وأفضل الممارسات	تحديد معايير الأمن التقني للشبكات والتطبيقات وإدارة الهوية والتشفير: • معايير أمن الشبكات والاتصالات • معايير أمن التطبيقات وقواعد البيانات • إدارة الهوية والوصول(IAM) ومعاييرها • معايير التشفير وحماية البيانات
	الاستجابة للحوادث السيبرانية واستمرارية الأعمال	تحديد معايير وخطط الاستجابة للحوادث وكيفيات التعافي: • معايير الاستجابة للحوادث السيبرانية • خطط استمرارية الأعمال والتعافي من الكوارث BC/DR
تدقيق الأمن السيبراني والامتثال للمعايير والتوجهات المستقبلية	تدقيق الأمن السيبراني والامتثال للمعايير	التدقيق والامتثال للمعايير: • تدقيق الأمن السيبراني • الامتثال للمعايير

	التحديات المستقبلية والتوجهات الجديدة في الأمن السيبراني	التحديات المستقبلية والتوجهات الجديدة في الأمن السيبراني: • التحديات المستقبلية في الأمن السيبراني • التوجهات الجديدة في الأمن السيبراني

التمرين الشامل

أنت مدير الأمن السيبراني في بنك جزائري. البنك يقوم بتطوير نظام جديد للمعاملات المصرفية عبر الإنترنت. يتطلب هذا النظام حماية قصوى لبيانات العملاء المالية والشخصية (أرقام الحسابات، أرصدة، معلومات الهوية).

المطلوب:

- حدد التقنيات والمعايير الأساسية (من التشفير، التجزئة، التوقيعات/الشهادات الرقمية) التي ستطبقها لضمان:
  - ✓ سرية بيانات العملاء أثناء تخزينها في قاعدة البيانات.
  - ✓ سرية الاتصالات بين العميل وخادم البنك عبر الإنترنت.
  - ✓ تكاملية بيانات المعاملات المالية (للتأكد من عدم التلاعب بالمبالغ أو المستفيدين).
  - ✓ مصادقة هوية العميل عند تسجيل الدخول.
  - ✓ عدم تنصل العميل من المعاملات التي قام بها.
- اشرح باختصار كيف تساهم كل تقنية مختارة في تحقيق الهدف الأمني المحدد.
- اذكر اثنين من أفضل الممارسات الإضافية التي ستطبقها لتعزيز حماية هذا النظام.

الملاحق

حل التمرين الشامل

- تحديد التقنيات والمعايير الأساسية (من التشفير، التجزئة، التوقيعات/الشهادات الرقمية)
  - سرية البيانات المخزنة: تطبيق تشفير متماثل قوي مثل AES-256 على قاعدة البيانات التي تحتوي على بيانات العملاء المالية والشخصية. استخدام أنظمة إدارة مفاتيح آمنة لضمان سرية المفاتيح نفسها.
  - سرية الاتصالات: استخدام بروتوكول TLS/SSL (HTTPS) بين متصفح العميل وخادم البنك. يتم ذلك بتبادل مفاتيح متماثلة باستخدام RSA أو ECC ثم تشفير البيانات باستخدام AES، مما يضمن سرية البيانات أثناء النقل.
  - تكاملية المعاملات: استخدام وظائف التجزئة مثل SHA-256 لحساب قيمة تجزئة لكل معاملة مالية قبل تخزينها أو إرسالها. عند الحاجة للتحقق، يتم إعادة حساب التجزئة ومقارنتها بالقيمة المخزنة للتأكد من عدم التلاعب بالبيانات. يمكن أيضًا استخدام التوقيعات الرقمية للتحقق من سلامة أوامر المعاملات.
  - مصادقة هوية العميل: استخدام مزيج من اسم المستخدم وكلمة مرور قوية (مخزنة كقيم تجزئة مع الملح) بالإضافة إلى المصادقة متعددة العوامل (MFA) مثل رموز OTP المرسلة عبر الرسائل القصيرة أو تطبيقات المصادقة. استخدام الشهادات الرقمية للخادم للتحقق من هوية البنك للعميل.
  - عدم تنصل العميل: يمكن تفعيل التوقيعات الرقمية على المعاملات الكبيرة أو الحساسة. يقوم العميل بتوقيع المعاملة رقميًا باستخدام مفتاحه الخاص (بعد مصادقته)، مما يوفر دليلًا غير قابل للإنكار على إجرائه للمعاملة. يتطلب هذا بنية تحتية للمفاتيح العامة (PKI) للعملاء أو استخدام آليات توقيع مبنية على البنك نفسه.
- الممارسات الإضافية:
  - تطبيق سياسات كلمات مرور صارمة (طول، تعقيد، تغيير دوري)،
  - التحكم في الوصول بناءً على مبدأ أقل امتياز للموظفين،
  - المراقبة المستمرة لسجلات الأمان وكشف التهديدات،
  - إجراء تدقيقات أمنية واختبارات اختراق منتظمة Penetration Testing لضمان فعالية الإجراءات الأمنية.