الدورة التدريبية: قانون الجرائم السيبرانية وتحديات الأمن الرقمي والمسؤولية القانونية

#LEG1740

الدورة التدريبية: قانون الجرائم السيبرانية وتحديات الأمن الرقمي والمسؤولية القانونية

مقدمة الدورة التدريبية / لمحة عامة:

يقدم BIG BEN Training Center هذه الدورة التدريبية المتخصصة في قانون الجرائم السيبرانية، والتي صُممت لتزويد المشاركين بفهم عميق للتحديات القانونية والأمنية المرتبطة بالعالم الرقمي المتزايد التعقيد. في عصر التحول الرقمي، أصبحت الجرائم السيبرانية تهديدًا متزايدًا للأفراد والمؤسسات والدول على حد سواء، مما يستدعي معرفة متقدمة بالتشريعات المنظمة لها وكيفية التعامل معها. تتناول الدورة بالتفصيل أنواع الجرائم السيبرانية، والإطار القانوني الوطني والدولي لمكافحتها، بالإضافة إلى تحديات الأمن الرقمي والمسؤولية القانونية المترتبة على الأفراد والكيانات. كما يؤكد الأكاديمي البارز البروفيسور دانييل سولوف (Professor Daniel J. Solove) في أبحاثه حول قانون الخصوصية والأمن السيبراني، فإن فهم الجوانب القانونية للجرائم السيبرانية أمر بالغ الأهمية لحماية البيانات والبنى التحتية الحيوية. تركز هذه الدورة على تزويد المشاركين بالمهارات العملية اللازمة لـتحديد المخاطر السيبرانية، وتطبيق إجراءات الحماية القانونية، والتعامل مع الاختراقات الأمنية، وتحديد المسؤولية القانونية في حالات الجرائم الإلكترونية. تهدف الدورة إلى تمكين المختصين من بناء استراتيجيات دفاعية قوية، مما يساهم في حماية الأصول الرقمية وضمان الامتثال القانوني.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- المستشارون القانونيون ومحامو الجرائم السيبرانية.
- مسؤولو الأمن السيبراني وتقنية المعلومات.
- المديرون التنفيذيون في الشركات التقنية والمالية.
- مديرو الامتثال والمخاطر.
- المحققون في الجرائم الإلكترونية.
- القضاة وأعضاء النيابة العامة المتخصصون.
- مسؤولو حماية البيانات والخصوصية.

القطاعات والصناعات المستهدفة:

- القطاع الحكومي والجهات الأمنية.
- القطاع المالي والمصرفي.
- شركات الاتصالات وتقنية المعلومات.
- شركات التجارة الإلكترونية.
- قطاع الرعاية الصحية.
- شركات المحاماة والاستشارات القانونية.
- شركات البنية التحتية الحيوية.

الأقسام المؤسسية المستهدفة:

- الإدارات القانونية.
- إدارات الأمن السيبراني.
- إدارات تقنية المعلومات.
- إدارات الامتثال.
- إدارات المخاطر.
- إدارات التدقيق الداخلي.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم عميق لمفهوم الجرائم السيبرانية وأنواعها.
- تحديد الإطار القانوني لمكافحة الجرائم السيبرانية على المستويين الوطني والدولي.
- تطبيق مبادئ الأمن الرقمي لحماية الأنظمة والبيانات.
- تقييم المسؤولية القانونية في حالات الاختراقات الأمنية.
- التعامل مع الأدلة الرقمية والتحقيقات الجنائية الإلكترونية.
- صياغة سياسات وإجراءات الامتثال لقوانين الجرائم السيبرانية.
- تطوير استراتيجيات فعالة للدفاع ضد التهديدات السيبرانية.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة منهجية تدريبية متكاملة تجمع بين المعرفة القانونية المتعمقة في قانون الجرائم السيبرانية والتطبيقات العملية للأمن الرقمي، لضمان تزويد المشاركين بالمهارات اللازمة للتعامل مع التحديات الأمنية والقانونية في الفضاء السيبراني. يتم تقديم المحتوى من خلال محاضرات تفاعلية يقودها خبراء في القانون السيبراني، ومتخصصون في الأمن السيبراني، تليها جلسات نقاش وحوارات معمقة تتيح للمشاركين تبادل الخبرات والتحديات. تُستخدم دراسات حالة واقعية لجرائم سيبرانية حدثت في مختلف القطاعات، بالإضافة إلى أمثلة على الإجراءات الوقائية، مما يوفر للمتدربين فرصة لتحليل السيناريوهات المعقدة وتطوير حلول قانونية وأمنية. تتضمن الدورة ورش عمل تطبيقية مكثفة، حيث يتدرب المشاركون على تحديد نقاط الضعف الأمنية، وتحليل الثغرات القانونية، ووضع خطط الاستجابة للحوادث السيبرانية. يتم تشجيع العمل الجماعي لتعزيز مهارات التعاون والتفكير النقدي في حل المشكلات. تُقدم تغذية راجعة بناءة ومستمرة لضمان فهم شامل للمفاهيم وتطوير المهارات. تهدف هذه المنهجية إلى تمكين المشاركين من حماية الأصول الرقمية لمؤسساتهم والوفاء بالتزاماتهم القانونية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: الإطار القانوني للجرائم السيبرانية

- مفهوم الجرائم السيبرانية وأنواعها.
- التشريعات الدولية والاتفاقيات المتعلقة بالجرائم الإلكترونية.
- القوانين الوطنية لمكافحة الجرائم السيبرانية.
- جرائم الدخول غير المصرح به (الاختراق).
- جرائم التخريب والاعتداء على البيانات والأنظمة.
- الاحتيال الإلكتروني وسرقة الهوية.
- جرائم المحتوى غير المشروع على الإنترنت.

الوحدة الثانية: الأمن الرقمي وحماية البيانات

- مبادئ الأمن الرقمي الأساسية.
- حماية البنى التحتية الحيوية.
- أمن الشبكات والخوادم.
- تشفير البيانات وحماية الخصوصية.
- الاستجابة للحوادث الأمنية والاختراقات.
- أهمية التوعية والتدريب في الأمن الرقمي.
- دور تقييم المخاطر الأمنية.

الوحدة الثالثة: المسؤولية القانونية في الجرائم السيبرانية

- المسؤولية القانونية الجنائية في الجرائم السيبرانية.
- المسؤولية القانونية المدنية عن الأضرار السيبرانية.
- مسؤولية مزودي الخدمات الإلكترونية.
- مسؤولية الشركات عن أمن البيانات.
- مسؤولية الموظفين عن المخالفات السيبرانية.
- قوانين حماية البيانات والخصوصية (GDPR وغيرها).
- حدود المسؤولية القانونية في الفضاء السيبراني.

الوحدة الرابعة: التحقيقات الجنائية الرقمية والأدلة الإلكترونية

- مفهوم التحقيق الجنائي الرقمي (Digital Forensics).
- جمع الأدلة الرقمية بطرق قانونية.
- حفظ الأدلة وسلسلة الحضانة الرقمية.
- تحليل الأدلة الرقمية واستخراج المعلومات.
- التقارير الفنية للأدلة الرقمية.
- تحديات قبول الأدلة الرقمية في المحاكم.
- دور الخبراء الفنيين في التحقيقات السيبرانية.

الوحدة الخامسة: التحديات المستقبلية والوقاية

- تحديات الذكاء الاصطناعي في الجرائم السيبرانية.
- جرائم العملات المشفرة والبلوك تشين.
- الأمن السيبراني في إنترنت الأشياء (IoT).
- التعاون الدولي في مكافحة الجريمة السيبرانية.
- التطورات التشريعية المستقبلية في القانون السيبراني.
- بناء ثقافة الأمن الرقمي في المؤسسات.
- الوقاية الاستباقية من التهديدات السيبرانية.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20–25 ساعة تدريبية.

سؤال للتأمل:

في ظل التطور المتسارع للتكنولوجيا والتهديدات السيبرانية، كيف يمكن للمشرعين والمؤسسات القانونية مواكبة هذه التحديات المتغيرة باستمرار لضمان بيئة رقمية آمنة، مع الحفاظ على التوازن بين حماية الأمن الوطني وحقوق الأفراد والابتكار التكنولوجي؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل على قانون الجرائم السيبرانية، وتقديم نهج متكامل يجمع بين تحديات الأمن الرقمي والمسؤولية القانونية. نذهب أبعد من مجرد شرح القوانين، حيث نقدم للمشاركين استراتيجيات عملية لـتحديد المخاطر السيبرانية، وتطبيق إجراءات الحماية القانونية، والتعامل مع الاختراقات الأمنية. ما يميز هذه الدورة حقًا هو المحتوى المتقدم الذي يتضمن دراسات حالة واقعية وورش عمل تطبيقية مكثفة حول التحقيقات الجنائية الرقمية وتحديد المسؤولية القانونية. يتم تقديم المحتوى من قبل خبراء في القانون السيبراني والأمن السيبراني، مما يضمن حصول المشاركين على رؤى عملية قابلة للتطبيق. هذه الدورة ليست مجرد تدريب نظري، بل هي فرصة لـإتقان المهارات اللازمة لحماية الأصول الرقمية للمؤسسات والوفاء بالالتزامات القانونية، مما يجعلها ضرورية لأي مهني يسعى للتميز في هذا المجال الحيوي.