الدورة التدريبية: قانون الجرائم السيبرانية وتحديات الأمن الرقمي والمسؤولية القانونية

يوليو ٢٠٢٦ ٣١ - ٢٧

باكو - *

(للشخص الواحد) € ٥٠٠٠

Ref: #LEG1740_236819

مقدمة الدورة التدريبية / لمحة عامة:

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

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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: الإطار القانوني للجرائم السيبرانية

- مفهوم الجرائم السيبرانية وأنواعها.
- الإلكترونية. التشريعات الدولية والاتفاقيات المتعلقة بالجرائم
- 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.

السيبرانية الوحدة الثالثة: المسؤولية القانونية في الجرائم

- السيبرانية. المسؤولية القانونية الجنائية في الجرائم
- السيبرانية. المسؤولية القانونية المدنية عن الأضرار
- 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.

والأدلة الإلكترونية الوحدة الرابعة: التحقيقات الجنائية الرقمية

- 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.
- السيبراني. التطورات التشريعية المستقبلية في القانون
- بناء ثقافة الأمن الرقمي في المؤسسات.
- الوقاية الاستباقية من التهديدات السيبرانية.

الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام، ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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