QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1732

دورة الأمن السيبراني والحماية من البيانات في الحكومة الرقمية

الحكومة الرقمية والحكومة الذكية
الحكومة والقطاع العام

المدة
5 أيام

طريقة التقديم
حضوري

نظرة عامة على الدورة

تقدم دورة الأمن السيبراني والحماية من البيانات في الحكومة الرقمية إطاراً استراتيجياً وعملياً متكاملاً لحماية الخدمات الحكومية الرقمية والأنظمة المعلوماتية والأصول الرقمية والبيانات الحكومية وبيانات المستفيدين من المخاطر والتهديدات السيبرانية المتطورة. وتهدف الدورة إلى تمكين الوزارات والجهات الحكومية ومؤسسات القطاع العام من تعزيز المرونة السيبرانية وحماية البيانات، مع الحفاظ على خدمات رقمية آمنة وموثوقة ومستدامة.

يؤدي التوسع في الخدمات الحكومية الرقمية إلى زيادة حجم البيانات الحكومية وحساسيتها وترابط الأنظمة والمنصات الرقمية. ولذلك تحتاج الجهات الحكومية إلى إدارة المخاطر المرتبطة بالمنصات والتطبيقات والشبكات والبيئات السحابية والأنظمة المتصلة والموظفين والأطراف الخارجية ومقدمي الخدمات. ويتطلب ذلك منهجية متكاملة تجمع بين الحوكمة وإدارة المخاطر والضوابط التقنية وحماية البيانات ورفع الوعي والاستجابة للحوادث والمراقبة المستمرة.

يغطي البرنامج المبادئ الأساسية للأمن السيبراني والحماية من البيانات في بيئة الحكومة الرقمية، بما يشمل حوكمة الأمن السيبراني، وتقييم مخاطر أمن المعلومات، وتصنيف البيانات، وإدارة الهوية والوصول، والتشفير، وتأمين الخدمات الرقمية، وأمن الحوسبة السحابية، وحماية الخصوصية، وإدارة مخاطر الأطراف الثالثة، والمراقبة الأمنية. كما يتناول الأساليب العملية لحماية البيانات طوال دورة حياتها، بدءاً من جمعها وتخزينها ومعالجتها ومشاركتها ووصولاً إلى الاحتفاظ بها والتخلص الآمن منها.

ويركز البرنامج بصورة خاصة على إدارة الحوادث السيبرانية وحماية الخدمات الحكومية الحيوية من التعطيل والوصول غير المصرح به وفقدان البيانات والاحتيال وغيرها من التهديدات الرقمية. كما يتناول الاستجابة للحوادث واستمرارية الأعمال والتعافي من الكوارث وإدارة الثغرات ورفع الوعي الأمني وتعزيز المرونة السيبرانية للمؤسسة.

ومن خلال التمارين التطبيقية والسيناريوهات الحكومية وتقييم المخاطر وتقييمات حماية البيانات ومحاكاة الاستجابة للحوادث ومراجعة الضوابط الأمنية والتخطيط للتنفيذ، يطور المشاركون القدرات اللازمة لتعزيز الأمن السيبراني للحكومة الرقمية وتطبيق ممارسات عملية لحماية البيانات ودعم خدمات حكومية رقمية آمنة ومرنة وموثوقة.

أهداف الدورة

- تحليل تحديات الأمن السيبراني المرتبطة بالتحول نحو الحكومة الرقمية.
- تقييم مخاطر الأمن السيبراني وحماية البيانات في الأنظمة والخدمات والتطبيقات والأصول المعلوماتية الحكومية.
- تطوير منهجيات لحوكمة الأمن السيبراني بما يتوافق مع الأهداف المؤسسية ومتطلبات الحكومة الرقمية.
- تطبيق مبادئ تصنيف البيانات وحمايتها طوال دورة حياة المعلومات.
- تقييم ضوابط الهوية وإدارة الوصول والمصادقة والتفويض وإدارة صلاحيات الوصول المميزة.
- تقييم متطلبات الأمن للخدمات والمنصات والتطبيقات الحكومية والبيئات السحابية والأنظمة المتصلة.
- تطبيق أساليب عملية لحماية البيانات الحساسة والشخصية من الوصول أو الاستخدام غير المصرح به.
- تطوير إجراءات الاستجابة للحوادث السيبرانية والتصعيد والتواصل في البيئة الحكومية.
- تقييم مخاطر الأمن السيبراني المرتبطة بالموردين والمتعاقدين ومقدمي الخدمات والأطراف الثالثة.
- تصميم مبادرات لرفع الوعي الأمني وبناء قدرات القوى العاملة وتعزيز المرونة السيبرانية.
- تطوير مؤشرات أداء لمتابعة فعالية الأمن السيبراني وحماية البيانات.
- تعزيز قدرات استمرارية الأعمال والتعافي من الكوارث والمرونة السيبرانية.
- إعداد خارطة طريق عملية لتحسين الأمن السيبراني وحماية البيانات في الخدمات الحكومية الرقمية.

الفئة المستهدفة

تستهدف هذه الدورة القيادات الحكومية والتنفيذية ومديري تقنية المعلومات والأمن السيبراني وأمن المعلومات ومتخصصي حماية البيانات والخصوصية ومديري تكنولوجيا المعلومات وقادة التحول الرقمي ومتخصصي المخاطر والامتثال والمراجعة الداخلية ومديري الخدمات الحكومية الرقمية.

وتناسب الدورة بصورة خاصة الوزارات والهيئات الحكومية ومؤسسات القطاع العام المسؤولة عن تشغيل المنصات

الحكومية الرقمية والخدمات الإلكترونية وقواعد البيانات والبيئات السحابية وأنظمة المعلومات والتطبيقات الموجهة للمواطنين والبنية التحتية الرقمية الحيوية.

كما يستفيد من البرنامج مديرو البيانات ومسؤولو الأنظمة والشبكات والأمن السيبراني وفرق التطبيقات والبنية التحتية ومتخصصو استمرارية الأعمال والتعافي من الكوارث ومتخصصو المشتريات وإدارة مخاطر الأطراف الثالثة والفرق القانونية وفرق الامتثال وصناع القرار المسؤولون عن حوكمة الأمن السيبراني وحماية البيانات واستمرارية الخدمات الرقمية.

مخرجات التعلم

- شرح تحديات الأمن السيبراني وحماية البيانات المرتبطة بالحكومة الرقمية.
- تقييم المخاطر السيبرانية التي تؤثر على الأنظمة والتطبيقات والخدمات والأصول المعلوماتية الحكومية.
- تطوير هيكل عملي لحوكمة الأمن السيبراني في بيئة الحكومة الرقمية.
- تصنيف البيانات الحكومية وفق درجة حساسيتها وأهميتها ومتطلبات حمايتها.
- تطبيق ضوابط حماية البيانات طوال دورة حياة المعلومات.
- تقييم ضوابط إدارة الهوية والوصول والمصادقة والتفويض وإدارة الصلاحيات المميزة.
- تحديد متطلبات الأمن للتطبيقات والخدمات الحكومية والبيئات السحابية والشبكات والأنظمة المتصلة.
- تقييم مخاطر الخصوصية وحماية البيانات الناتجة عن جمع المعلومات ومعالجتها وتخزينها ومشاركتها.
- تطوير إجراءات عملية للاستجابة للحوادث السيبرانية والتصعيد وإدارة الأزمات.
- تقييم المخاطر السيبرانية المرتبطة بالموردين والمتعاقدين ومقدمي الخدمات والأطراف الثالثة.
- تصميم مبادرات لرفع الوعي السيبراني وتقليل المخاطر المرتبطة بالعامل البشري.
- تطوير مؤشرات أداء ومؤشرات مخاطر لمتابعة الأمن السيبراني وحماية البيانات.
- تعزيز خطط استمرارية الأعمال والتعافي من الكوارث والمرونة السيبرانية.

- إعداد خارطة طريق عملية لتحسين الأمن السيبراني وحماية البيانات في الخدمات الحكومية الرقمية.
- المحاور التدريبية:

محاور الدورة

اليوم الأول

أسس الأمن السيبراني وإدارة المخاطر في الحكومة الرقمية

- الأمن السيبراني في بيئة الحكومة الرقمية
- التهديدات السيبرانية المتطورة التي تستهدف الخدمات الحكومية
- أسطح الهجوم والأصول المعلوماتية والرقمية الحيوية
- حوكمة الأمن السيبراني والمسؤوليات والمساءلة المؤسسية
- تحديد وتقييم وترتيب أولويات مخاطر الأمن السيبراني
- تحديد الخدمات والأنظمة والتطبيقات والمعلومات الحرجة
- التطبيق العملي: إجراء تقييم لمخاطر الأمن السيبراني لخدمة حكومية رقمية مختارة

اليوم الثاني

حماية البيانات والخصوصية وأمن المعلومات

- مبادئ حماية البيانات ومتطلبات أمن المعلومات
- تصنيف البيانات الحكومية وطرق التعامل معها
- إدارة دورة حياة البيانات وضوابط الحماية
- حماية البيانات الشخصية والسرية والحساسة
- الوصول إلى البيانات ومشاركتها والاحتفاظ بها والتخلص الآمن منها

اليوم الثاني — تابع

- التشفير والتخزين الآمن ونقل البيانات
- التطبيق العملي: إعداد إطار لتصنيف وحماية أحد أصول البيانات الحكومية

اليوم الثالث

تأمين الخدمات الرقمية وإدارة الهوية والأمن السحابي

- الأمن منذ مرحلة التصميم للخدمات الحكومية الرقمية
- إدارة الهوية والوصول
- المصادقة والتفويض وإدارة الصلاحيات المميزة
- أمن التطبيقات والشبكات والأجهزة الطرفية
- متطلبات أمن الحوسبة السحابية في البيئة الحكومية
- إدارة الثغرات والاختبارات الأمنية والمراقبة المستمرة
- التطبيق العملي: تقييم البنية الأمنية وضوابط الوصول لخدمة حكومية رقمية

اليوم الرابع

الاستجابة للحوادث السيبرانية والمرونة المؤسسية

- تحديد وتصنيف الحوادث السيبرانية
- أدوار ومسؤوليات وإجراءات الاستجابة للحوادث
- التواصل والتصعيد وإدارة الحوادث السيبرانية
- خروقات البيانات والوصول غير المصرح به والبرمجيات الخبيثة والتصيد وتعطيل الخدمات
- المراقبة الأمنية واكتشاف التهديدات
- استمرارية الأعمال والتعافي من الكوارث للخدمات الحكومية الرقمية
- مخاطر الأطراف الثالثة وسلسلة التوريد الرقمية

اليوم الرابع — تابع

- التطبيق العملي: تنفيذ محاكاة للاستجابة لحادث سيبراني في بيئة حكومية

اليوم الخامس

المرونة السيبرانية والحوكمة وخارطة طريق حماية البيانات

- مؤشرات أداء الأمن السيبراني وحماية البيانات
- المراقبة الأمنية وإعداد التقارير ولوحات المتابعة
- تقييم نضج المرونة السيبرانية والتحسين المستمر
- الوعي الأمني وبناء القدرات السيبرانية للقوى العاملة
- حوكمة الأمن السيبراني والضمان والمراجعة والامتثال
- تحديد الأولويات الاستراتيجية وتخطيط التنفيذ
- الورشة الختامية: إعداد خارطة طريق متكاملة للأمن السيبراني وحماية البيانات في الحكومة الرقمية تشمل الحوكمة، وتقييم المخاطر، وتصنيف البيانات، والخصوصية، وإدارة الهوية والوصول، وتأمين الخدمات الرقمية، وأمن الحوسبة السحابية، والاستجابة للحوادث، واستمرارية الأعمال، وإدارة مخاطر الأطراف الثالثة، والوعي الأمني، وقياس الأداء، والمرونة السيبرانية، والتحسين المستمر.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

https://quest-training.com/courses/digital-government-cybersecurity-data-protection-training-course

الموقع الإلكتروني: https://quest-training.com

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440