# مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

# الحوسبة السحابية وتأمين البنية التحتية الحكومية

مكان الإنعقاد : الإمارات العربية المتحدة – دبي

تاريخ الإنعقاد : 16– 20/ 11 / 2025.

## مقدمة :

في عصر التحول الرقمي المتسارع، تلعب الحوسبة السحابية دورًا محوريًا في تحسين كفاءة العمليات الحكومية وتخزين البيانات ومعالجتها بشكل آمن وفعّال. توفر الحوسبة السحابية للجهات الحكومية القدرة على تقليل التكاليف التشغيلية، تسريع الابتكار، وتحسين الخدمات المقدمة للمواطنين. ومع ذلك، تأتي هذه الفوائد مع تحديات كبيرة تتعلق بتأمين البنية التحتية السحابية وحماية البيانات الحساسة. يهدف برنامج "الحوسبة السحابية وتأمين البنية التحتية الحكومية" إلى تزويد المشاركين بالمعرفة والأدوات اللازمة لفهم كيفية تطبيق الحوسبة السحابية بشكل آمن في المؤسسات الحكومية، وضمان حماية البنية التحتية الرقمية من الهجمات الإلكترونية والمخاطر الأمنية.

## أهداف الورشة:

- فهم المفاهيم الأساسية للحوسبة السحابية ونماذج الخدمة المختلفة (IaaS، PaaS، SaaS).
- تحديد الفوائد والتحديات الأمنية المرتبطة بتبني الحوسبة السحابية في القطاع الحكومي.
- تطوير استراتيجيات فعالة لتأمين البنية التحتية الحكومية في بيئة السحابة.
- فهم مبادئ أمن المعلومات وتطبيقها في سياق الحوسبة السحابية.
- استكشاف التقنيات والأدوات الحديثة المستخدمة في تأمين الحوسبة السحابية.
- بناء القدرات على تقييم المخاطر الأمنية وإدارة الحوادث في بيئة السحابة.
- تطوير خطط استجابة فعالة للحوادث الأمنية في الحوسبة السحابية.

## محتويات الورشة:

### اليوم التدريبي الأول:

**مقدمة في الحوسبة السحابية**

- تعريف الحوسبة السحابية ونماذج الخدمة المختلفة (IaaS، PaaS، SaaS).
- فوائد وتحديات تبني الحوسبة السحابية في القطاع الحكومي.
- استعراض أنواع السحابة (عامة، خاصة، هجينة).
- مناقشة أفضل الممارسات في اختيار مزود خدمة سحابية.

## اليوم التدريبي الثاني:

**أمن الحوسبة السحابية**

- مبادئ أمن المعلومات وتطبيقها في سياق الحوسبة السحابية.
- تحديد المخاطر الأمنية الشائعة في بيئة السحابة (مثل الوصول غير المصرح به، فقدان البيانات، هجمات الحرمان من الخدمة).
- استراتيجيات لتأمين البيانات والأنظمة الحكومية في السحابة.
- دور التشفير وإدارة الهوية والوصول في أمن الحوسبة السحابية.

## اليوم التدريبي الثالث:

**التقنيات والأدوات في أمن الحوسبة السحابية**

- استكشاف التقنيات والأدوات الحديثة المستخدمة في تأمين الحوسبة السحابية (مثل جدران الحماية السحابية، أنظمة الكشف عن التسلل، إدارة الثغرات الأمنية).
- تطبيق هذه التقنيات والأدوات في سيناريوهات واقعية.
- مناقشة أهمية التحديثات الأمنية المستمرة والمراقبة الدورية.

## اليوم التدريبي الرابع:

**إدارة المخاطر الأمنية والاستجابة للحوادث**

- بناء القدرات على تقييم المخاطر الأمنية في بيئة السحابة.
- تطوير خطط استجابة فعالة للحوادث الأمنية.
- إجراء تدريبات على التعامل مع الحوادث الأمنية.
- أهمية التعاون والتنسيق بين مختلف الجهات المعنية في حالة وقوع حادث أمني.

## اليوم التدريبي الخامس:

**ورشة عمل وتطبيق عملي**

- ورشة عمل لتطبيق المفاهيم والمهارات المكتسبة على سيناريوهات واقعية.
- استخدام أدوات وتقنيات أمن الحوسبة السحابية.
- تقييم المخاطر الأمنية في بيئة سحابية افتراضية.
- تطوير خطة استجابة لحادث أمني افتراضي.
- جلسة نقاش مفتوحة حول مستقبل أمن الحوسبة السحابية في القطاع الحكومي.

## أساليب التدريب :

- نقاشات مفتوحة لتحليل وجهات النظر.
- دراسة حالات.
- قصص وأمثلة واقعية .
- التمارين واختبارات الشخصية.
- العصف الذهني.
- تكليف المتدربين بمشروعات جماعية أو فردية.
- ربط المحتوى بتجارب مألوفة.