مرونة الأعمال السيبرانية (Cyber Resilience)
والتعافي من الكوارث

الإمارات العربية المتحدة - دبي

2026 / 12 /03 – 11/29

مقدمة:

في عام 2026، لم يعد السؤال "هل سنتمكن من منع الهجوم؟" بل "ما مدى سرعة عودتنا للعمل بعد وقوعه؟". إن مرونة الأعمال السيبرانية هي الفن القيادي لتحويل الأزمات إلى فرص لإثبات قوة المنظومة الوطنية. يهدف هذا البرنامج إلى تمكين القادة من أدوات "الصمود الرقمي"، وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في خطط الاستمرارية، مع ضمان النزاهة المطلقة والسيادة على عمليات التعافي، مما يرسخ مكانة الدولة كبيئة أعمال لا تقبل التوقف تحت أي ظرف.

أهداف الدورة:

- استيعاب مفاهيم "الصمود السيادي" وعلاقتها باستمرارية الأعمال وتصفير البيروقراطية.
- تطوير مهارات هندسة "التعافي الذاتي (Self-Healing Systems) "لضمان استجابة الأنظمة اللحظية.
- إتقان فن إدارة "التوائم الرقمية (Digital Twins) "لمحاكاة الكوارث واختبار الجاهزية بنزاهة.
- حوكمة ممارسات "المرونة القطاعية" لضمان التنسيق الرشيق بين الجهات الحكومية والخاصة.
- تعزيز السيادة المعلوماتية عبر بناء "أنظمة نسخ احتياطي سيادية" مستقلة عن السحب الدولية.
- تطبيق استراتيجيات القيادة في إدارة "سمعة المؤسسة" أثناء التعافي وضمان المصداقية العالمية.

محتويات الورشة:

اليوم الأول :

فلسفة "الصمود السيادي" والرشاقة في إدارة الأزمات الرقمية

هندسة الحصانة الوطنية وتصفير البيروقراطية في خطط الاستمرارية

- مفهوم المرونة السيبرانية 2026 وأثره على السيادة الوطنية وجودة الحياة والنمو والتميز العالمي.
- مواءمة استراتيجيات المرونة مع مبدأ تصفير البيروقراطية عبر أتمتة "تحليل الأثر على الأعمال.(BIA) "
- تحليل العلاقة بين "سرعة التعافي" وبين بناء الثقة والمصداقية الدولية في المنظومة الحكومية.
- تمرين هندسة الاستباقية لتصميم ميثاق مرونة يصفّر زمن "اتخاذ قرار التفعيل" بنزاهة وشفافية.

قيادة النزاهة في حوكمة "البقاء الرقمي" والريادة الوطنية الشاملة

- تعزيز السيادة على منصات إدارة الأزمات لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في الكشف عن "أضرار الأزمة."
- بناء ثقافة "المرونة كمسؤولية وطنية" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل والنمو.
- صياغة ميثاق أخلاقيات قائد المرونة السيبرانية لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة التعافي بالذكاء الاصطناعي والتوائم الرقمية

تصفير زمن التعطل عبر الأنظمة ذاتية الإصلاح والمحاكاة الذكية

- توظيف الذكاء الاصطناعي في "التنبؤ بالفشل" قبل وقوعه وتصفير احتمالات التوقف المفاجئ بنزاهة.
- حماية "النسخ الاحتياطية السيادية" عبر تقنيات التخزين غير القابل للتغيير (Immutable Storage).
- تطبيق التوائم الرقمية (Digital Twins) لتصفير الهدر البيروقراطي في إجراءات اختبار التعافي الميداني.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لمؤشر "جاهزية التعافي."

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط أولويات الاستعادة

- إدارة المسؤولية البشرية القيادية عند استخدام الذكاء الاصطناعي في تحديد "الأنظمة الأهم للتعافي."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من تقارير "ما بعد الحادث" لضمان المصداقية والسيادة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات المرونة بنزاهة تامة والتميز.

اليوم الثالث :

هندسة "المرونة القطاعية" والحياد في إدارة الموارد والشمولية

تصفير البيروقراطية في "الدعم التبادلي بين الجهات" والشمولية الرقمية

- هندسة بروتوكولات التعاون القطاعي التي تصفّر زمن التنسيق في الأزمات الكبرى بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات تبادل المعلومات لضمان حياد النظم الرقمية والنمو والتميز.
- تطبيق تقنيات "سلاسل الكتل (Blockchain) "لتوثيق سجلات الاستجابة وتصفير احتمالات التلاعب بالسجلات.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني للقطاع لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي التكنولوجيا لضمان توافق خططهم مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي والاقتصادي للأعطال الرقمية لضمان النزاهة والعدالة والتميز.
- بناء سجلات نزاهة رقمية لكل عملية "محاكاة كارثة" كبرى لضمان الشفافية والوضوح والريادة والسيادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "المرونة والسمعة الوطنية" بأسلوب واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في لحظة الأزمة

القيادة الاتصالية وحماية السمعة الرقمية أثناء التعافي من الكوارث

- أخلاقيات التواصل في الأزمات السيبرانية المتسارعة والموازنة بين الإبهار والوقار السيادي والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة والفرق الفنية لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو.
- بناء أنظمة الإفصاح الاستباقي عن نجاحات "العودة للعمل" لتصفير فرص انتشار الشائعات والنزاهة التامة.
- التدقيق الأخلاقي على سلاسل توريد برمجيات التعافي لضمان خلوها من الممارسات الضارة والسيادة والريادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التي قد تهدد أمن بنك معلومات المرونة والسيادة والريادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "عملية التعافي" لضمان استعادة الثقة ببيانات صادقة ونزيهة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج الرصد ضد التلاعب الممنهج بالبيانات والواقع الرقمي.

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "الصامد" القدوة: من امتصاص الصدمات إلى هندسة الاستمرارية السيادية

هندسة "النبض الاستراتيجي" والرشاقة السيادية في مرونة الأعمال

- مصفوفة "النبض اللحظي" للتعافي التلقائي: تصميم نظام رصد سيادي يعتمد على التوائم الرقمية لتحويل بيانات "تحليل الأثر" إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن "بدء التعافي" وضمان أن الأنظمة ذاتية الإصلاح تباشر عملها بنزاهة ومصداقية تامة فور رصد أي اختلال في الخدمة.
- بروتوكول "الرشاقة السيادية" للاستمرارية الموزعة: هندسة مسار قرار "صفري الإجراءات" يسمح بتفعيل النسخ الاحتياطية السيادية فور رصد النبضة الاستراتيجية التي تشير إلى تعطل السحابة الرئيسية. يضمن هذا البروتوكول استمرارية تدفق الخدمات الحكومية دون قيود بيروقراطية أو انتظار للاعتمادات اليدوية التي تعطل نبض الأعمال في لحظات الكوارث.
- حوكمة "النزاهة في التعافي" والسيادة على النسخ: وضع ضوابط أخلاقية تضمن "عدم قابلية التغيير" للبيانات المستعادة، وتفعيل ميثاق "الصدق في تقارير ما بعد الحادث" لضمان استقلال القرار الوطني والوضوح التام أمام صانع القرار بشأن حصانة السمعة المؤسسية والسيادة المعلوماتية.
- مختبر "هندسة الحصانة ضد الانهيار الرقمي": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة كبرى" ناتجة عن تعطل خدمات الربط الدولي، وكيفية تفعيل "بروتوكولات الدعم التبادلي القطاعي" لحظياً لحماية جودة الحياة والنمو الوطني الشامل.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة منظومية تضمن نزاهة التعامل مع الأزمات والبيانات الوطنية بنسبة %.100
- القدرة على هندسة منظومات تعافي رشيقة وسيادية تتوافق مع متطلبات الريادة والتميز العالمية الشاملة.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي في النتائج.
- بناء سجل ممارسات فضلى في إدارة الذكاء الاستراتيجي للمرونة يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات العليا ومدراء استمرارية الأعمال، وإدارة المخاطر، والأمن السيبراني، والتميز المؤسسي.
- مسؤولو التخطيط الاستراتيجي وفرق تصفير البيروقراطية والتحول الرقمي في القطاعات الحيوية.
- خبراء الحوكمة والنزاهة والرقابة الإدارية المعنيون بضبط جودة الاستجابة للأزمات.
- رؤساء فرق المهام الخاصة ومحللو الكوارث السيبرانية في الهيئات الاتحادية والمحلية والوطنية.

أساليب التدريب:

يتم استخدام بعض من الأساليب التالية أو الكل حسب المتطلبات لكل تخصص :

- دراسة الحالة المعقدة (Complex Case Studies)
- المحاكاة والألعاب الاستراتيجية (Simulation and War Gaming)
- ورش العمل القائمة على التفكير التصميمي (Design Thinking Workshops)
- حلقات النقاش مع خبير من القطاعين العام أوالخاص.(Expert Panels)
- المختبرات التقنية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)