التخطيط المتكامل للاستعداد والاستجابة للطوارئ في المنشآت الحكومية

الإمارات العربية المتحدة - دبي

22 – 26/ 02 / 2026

مقدمة:

في إطار التوجه الاستراتيجي نحو السيادة الرقمية وتطبيق مبدأ تصفير البيروقراطية، لم يعد التخطيط للطوارئ مجرد ملفات ورقية تُحفظ في الأدراج، بل تحول إلى "منظومة استجابة ذكية" تعمل بدقة الخوارزميات وحكمة القيادة. تهدف هذه الدورة إلى تمكين القادة من بناء خطط متكاملة تدمج بين الجاهزية المادية والرشاقة الرقمية، لضمان استمرارية الأعمال وحماية الأصول السيادية. يركز البرنامج على حوكمة عمليات الطوارئ لضمان النزاهة المطلقة وتصفير زمن الاستجابة، مما يعزز ريادة الدولة وتميز منشآتها كبيئات آمنة ومحصنة رقمياً وإجرائياً.

أهداف الدورة:

- استيعاب مفاهيم **الجاهزية السيادية** وعلاقتها بالرشاقة المؤسسية وتصفير البيروقراطية في إدارة الأزمات.
- تطوير مهارات هندسة خطط الطوارئ المتكاملة التي تغطي السيناريوهات المادية والسيبرانية بنزاهة.
- إتقان فن تشغيل غرف عمليات الطوارئ الذكية باستخدام أنظمة المحاكاة والتحليل التنبؤي.
- حوكمة مسارات اتخاذ القرار أثناء الأزمات لضمان الشفافية والامتثال للتشريعات الوطنية والسيادية.
- اكتساب مهارات **تصفير الفجوة الزمنية (Zero Latency)** بين وقوع الحدث وبدء الاستجابة الفعالة.
- تعزيز السيادة الرقمية من خلال حماية قنوات الاتصال وأنظمة التحكم في المنشآت من الاختراق.
- تطبيق استراتيجيات "التعافي الرشيق" لضمان عودة الخدمات الحكومية للعمل في زمن قياسي.
- تطوير مهارات إدارة المعضلات الأخلاقية المرتبطة بتحديد الأولويات أثناء حالات الطوارئ الكبرى.
- صياغة خارطة طريق شاملة لتحويل المنشأة الحكومية إلى "حصن ذكي" يدعم جودة الحياة والريادة.

محتويات الورشة:

اليوم الأول:

فلسفة التخطيط المتكامل في عصر تصفير البيروقراطية

من "الخطط الساكنة" إلى "الاستجابة الديناميكية والرشاقة"

- مفهوم التخطيط المتكامل السيادي: كيف نصمم خططاً تتعلم وتتطور ذاتياً؟
- مواءمة الاستعداد مع استراتيجية تصفير البيروقراطية: إلغاء مسارات الاعتماد المعقدة أثناء الطوارئ.
- تحليل العلاقة بين "سرعة التبليغ الرقمي" وبين بناء الثقة والمصداقية الوطنية عالمياً.
- تمرين "هندسة السيناريو الصفري": تصميم نموذج استجابة يصفّر الخسائر البشرية والمادية إجرائياً.

النزاهة والسيادة في بناء "منظومة الجاهزية"

- مفهوم "السيادة السردية للأزمة": حماية الرواية الرسمية من التلاعب الرقمي أثناء الحادث.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة والقدوة الشخصية في الانضباط.
- سيكولوجية الثقة في الطوارئ: بناء المصداقية عبر "الصدق المعلوماتي" والعدالة في حماية الجميع.
- صياغة ميثاق "أخلاقيات المستجيب الأول" لضمان توافق الأداء مع القيم الوطنية والسيادية.

اليوم الثاني:

الهندسة التقنية لغرف عمليات الطوارئ الذكية

السيادة المعلوماتية والربط البيني لمحركات الاستجابة

- مكونات غرفة العمليات الذكية: دمج أنظمة المراقبة، المستشعرات، ومنصات التواصل بنزاهة.
- الأمان الرقمي كركيزة للاستعداد: حماية "أنظمة التحكم في المباني (BMS)" من الهجمات السيبرانية.
- إدارة الهوية الرقمية (UAE Pass) وأثرها على توثيق الوصول للمناطق الحساسة وتصفير الاختراقات.
- تمرين تقني: استخدام الذكاء الاصطناعي لمحاكاة إخلاء منشأة وتحديد نقاط الاختناق البيروقراطي.

أخلاقيات التفاعل مع أنظمة "القرار الآلي" في الطوارئ

- حدود استخدام الذكاء الاصطناعي في "أتمتة الإخلاء" دون فقدان الحكمة والمسؤولية البشرية.
- حوكمة مخرجات أنظمة "توزيع الموارد": الضمان الأخلاقي للعدالة في إنقاذ الأرواح بنزاهة.
- مفهوم "الأمانة في البيانات اللحظية": تجنب الاعتماد الكلي على الآلة في حالات "الهلوسة الرقمية."
- ورشة عمل: وضع ضوابط أخلاقية لاستخدام البيانات الضخمة في "توقع المخاطر المستقبلية للمنشأة."

اليوم الثالث:

الحياد والعدالة في إدارة الموارد والأزمات

النزاهة الرقمية ومكافحة الانحياز في توزيع المساعدات والإنقاذ

- أخلاقيات "العدالة في الاستجابة": ضمان وصول فرق الطوارئ لجميع النطاقات بنزاهة وشفافية.
- الرقابة الأخلاقية على أنظمة "تحديد الأولويات": كيف نضمن الشفافية في قرارات الحياة والموت؟
- تطبيق قاعدة "الإرادة البشرية القيادية": التدخل لتغيير مسار "استجابة آلية" قد تكون غير عادلة.
- حساب معامل الثقة في أنظمة الإنذار لتقليل احتمالات الخطأ الناتج عن "التنبيهات الكاذبة."

حوكمة المسؤولية عن مخرجات "أنظمة الحماية الذكية"

- المسؤولية المهنية للقائد عند حدوث "فشل في الاستجابة" ناتج عن أخطاء الأتمتة التقنية.
- إدارة العلاقة مع مزودي حلول "Emergency Tech": ضمان السيادة والشفافية في الخوارزميات.
- بناء أنظمة "التحقق المزدوج" لضمان عدم غياب الحكمة البشرية في القرارات المصيرية.
- تمرين محاكاة: إدارة أزمة تواصل ناتجة عن "عطل تقني" في أنظمة الإنذار وكيفية علاجه بنزاهة.

اليوم الرابع:

المسؤولية المهنية وإدارة السمعة السيادية في الأزمات

القيادة الاتصالية وحماية السمعة في بيئة هجينة

- أخلاقيات إدارة أزمات الطوارئ: الموازنة بين "سرعة الإفصاح" وبين الوقار والسيادة والخصوصية.
- الرقابة على "البصمة الرقمية للحادث" وأثرها على حيادية ومصداقية القرار السيادي والقانوني.
- بناء نظام "الإفصاح الاستباقي للدروس المستفادة": ضمان الشفافية لتصفير فرص انتشار الشائعات.
- التدقيق الأخلاقي على سلاسل "التوريد التقني للأمن" لضمان خلوها من الممارسات غير العادلة.

أخلاقيات الاستجابة للانتهاكات والاختراقات أثناء الطوارئ

- المسؤولية الأخلاقية في التبليغ عن الثغرات التي قد تؤدي لتعطيل "أنظمة الإطفاء أو الإنقاذ."
- فن التواصل الأخلاقي أثناء تعطل القنوات الرسمية: حماية الثقة عبر بيانات صادقة ونزيهة دون تضليل.
- إدارة "التعافي المؤسسي": إجراءات إعادة بناء الصورة بعد رصد انحراف في معايير الاستعداد الرقمي.
- بناء خطة "الحصانة الشاملة للمنشأة": تحصين منظومة الطوارئ ضد الهجمات أو الإهمال الممنهج.

اليوم الخامس:

هندسة الاستجابة الفورية وتصفير البيروقراطية في مواجهة حالات الطوارئ بالمنشآت الحكومية

مختبر "الضغط العالي" وإدارة الأزمات المتداخلة في المرافق السيادية

- محاكاة "سيناريو الانقطاع الشامل": وضع القادة في بيئة تحاكي تعطل الأنظمة الحيوية (الكهرباء، والاتصالات، وأنظمة التحكم) بالتزامن مع حادث أمني، واختبار قدرة الفرق على تفعيل بروتوكولات "العمل المستمر" بنزاهة ووضوح تام، مع الحفاظ على السيادة الرقمية ومنع التداخل الخارجي غير المصرح به.
- تصفير البيروقراطية في إدارة الموارد الاستعجالية: تطبيق مسار قرار "صفري الإجراءات" لتحريك فرق الإنقاذ وتوزيع الدعم التقني واللوجستي بناءً على تنبيهات الحساسات الذكية، لضمان حماية الأرواح والأصول دون قيود إدارية معطلة، مع ضمان الحصانة القانونية والنزاهة في كل خطوة تنفيذية.
- هندسة "القيادة الموزعة" تحت الأزمة: اختبار قدرة القائد على الموازنة بين "الاستجابة المؤتمتة" التي تطلقها غرف العمليات الذكية وبين "الحكمة البشرية" عند حدوث تعارض في البيانات الميدانية، لضمان استعادة السيطرة بنزاهة تامة ودون تعطيل جودة الحياة أو انسيابية الخدمات الأساسية في المنشأة.
- ورشة "تفكيك سجلات الاستجابة": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات التنبؤية، لتحديد الفجوات السلوكية في التنسيق بين القطاعات وتطوير حلول استباقية تمنع ارتباك الأنظمة في الواقع الميداني، مما يعزز ريادة الدولة في بناء "منشآت معصومة" من مفاجآت الأزمات.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية "حصانة مؤسسية" تضمن نزاهة التعامل مع الطوارئ بنسبة 100.%
- القدرة على هندسة منظومات استجابة "ذكية ومتكاملة" بمرونة وتوافق مع متطلبات السيادة.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي.
- بناء سجل ممارسات فضلى في إدارة استمرارية الأعمال يدعم اتخاذ القرار القيادي الآمن والمستدام.
- تحقيق جاهزية كاملة للمؤسسة والمسؤول للمنافسة في فئات التميز والريادة في الأمن والحوكمة.

الفئة المستهدفة:

- القيادات والمدراء في إدارات السلامة، إدارة الأزمات والكوارث، والخدمات المساندة.
- مسؤولو الأمن المؤسسي، مدراء المنشآت، وخبراء التحول الرقمي في الجهات السيادية.
- فرق الاستجابة للطوارئ، مسؤولو التميز المؤسسي، ومستشارو استمرارية الأعمال.
- رؤساء فرق مشاريع تصفير البيروقراطية وتطوير منظومات الحوكمة الرشيقة في قطاع الأمن والسلامة.
- الكوادر الطموحة الساعية لامتلاك جدارات "قائد الطوارئ والنزاهة الرقمية."

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)