القيادة الأمنية وإدارة المخاطر في المؤسسات

الإمارات العربية المتحدة - دبي

2026 / 11 /12 – 08

مقدمة:

تمثل القيادة الأمنية في العصر الرقمي الركيزة الأساسية لحماية مكتسبات الدولة وضمان استقرار جودة الحياة. لم يعد دور القائد الأمني مقتصرًا على الحماية المادية، بل امتد ليشمل قيادة التحول نحو بيئات عمل ذكية تصفّر البيروقراطية وتعتمد على السيادة المعلوماتية الكاملة. يهدف هذا البرنامج إلى تمكين القادة من أدوات إدارة المخاطر الاستباقية وتوظيف الذكاء الاصطناعي لتعزيز النزاهة والشفافية، مما يضمن ريادة المؤسسة وتحويل التحديات الأمنية إلى فرص لتعزيز التميز المؤسسي والسيادة الوطنية.

أهداف الدورة:

- استيعاب مفاهيم القيادة الأمنية الحديثة وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية.
- تطوير مهارات هندسة "مصفوفة المخاطر المؤسسية" باستخدام أدوات التحليل الرقمي التنبؤية.
- إتقان فن توظيف الذكاء الاصطناعي في حوكمة العمليات الأمنية لضمان النزاهة والشفافية.
- تعزيز السيادة المعلوماتية عبر بناء أطر حماية وطنية للأصول المؤسسية الكبرى.
- تطبيق استراتيجيات القيادة في إدارة الأزمات الأمنية وضمان المصداقية والسمعة المؤسسية.
- تمكين القادة من صياغة "ثقافة أمنية رشيقة" تدعم الابتكار والتميز في جودة الحياة.

محتويات الورشة:

اليوم الأول :

فلسفة القيادة الأمنية والسيادة في عصر الرشاقة

هندسة الأمن المؤسسي وتصفير البيروقراطية الإجرائية

- مفهوم القيادة الأمنية كدرع لحماية السيادة الوطنية وضمان جودة الحياة المؤسسية.
- مواءمة الاستراتيجية الأمنية مع مبدأ تصفير البيروقراطية عبر أتمتة الرقابة اللحظية.
- تحليل العلاقة بين "الأمن الرشيق" وبين بناء الثقة والمصداقية الدولية في النموذج الوطني.
- تمرين هندسة الاستجابة الاستباقية لتصميم دورة عمل تصفّر زمن اتخاذ القرار الأمني بنزاهة.

قيادة النزاهة في حوكمة الأصول والريادة الوطنية

- تعزيز السيادة على الأنظمة التقنية للأمن لضمان استقلاليتها وتوافقها مع القيم والهوية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في إدارة المخاطر والأزمات.
- بناء ثقافة "الأمان الممكن للابتكار" وعلاقتها بالنمو الاقتصادي السيادي والتميز الشامل.
- صياغة ميثاق أخلاقيات القائد الأمني لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة التقييم التنبؤي للمخاطر

تصفير مخاطر الاختراق عبر الذكاء الاصطناعي والتحليلات المتقدمة

- توظيف الذكاء الاصطناعي في رصد الأنماط غير الطبيعية وتصفير احتمالات التهديدات بنزاهة.
- حماية "البيانات الأمنية السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية المعلومات والنتائج.
- تطبيق الهوية الرقمية للأصول والأنظمة لتصفير الهدر البيروقراطي في إجراءات التدقيق والتحري.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لمؤشرات المخاطر.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط التهديدات

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في إصدار "تقدير الموقف."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في النتائج.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الذكاء الاصطناعي لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن القومي بنزاهة.

اليوم الثالث :

الحياد والعدالة في إدارة الأمن المجتمعي والشمولية

هندسة الحماية الشاملة والشمولية الرقمية في تغطية المجتمع

- استخدام التحليلات الذكية لضمان عدالة حماية جميع فئات المجتمع بنزاهة وشفافية مطلقة.
- تفعيل الرقابة الأخلاقية على منصات رصد التهديدات لضمان الشفافية وحياد البيانات الرقمية.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات الأمن التي قد تغفل البعد الإنساني.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع القطاع الخاص لضمان توافق الأنظمة الأمنية مع معايير جودة الحياة والسيادة.
- تطوير آليات رصد الأثر الاجتماعي للسياسات الأمنية لضمان النزاهة والعدالة في النتائج والتميز.
- بناء سجلات نزاهة رقمية لكل عملية أمنية كبرى لضمان الشفافية المطلقة والوضوح التام والريادة.
- تمرين محاكاة لإدارة حوار أمني حول "الأمن والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة في الأزمات الأمنية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل في الأزمات الأمنية المتسارعة والموازنة بين الإبهار والوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للالتزام الأمني وأثرها في تعزيز مصداقية القرار السيادي عالميًا والريادة.
- بناء أنظمة الإفصاح الاستباقي عن المخاطر المجهضة لضمان الشفافية وتصفير الشائعات الرقمية.
- التدقيق الأخلاقي على سلاسل توريد التقنيات الأمنية لضمان خلوها من الممارسات الضارة والنزاهة.

حصانة الأنظمة السيادية ضد الانتهاكات المعلوماتية والتلاعب

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات والسيادة.
- مهارات التواصل الأخلاقي عند حدوث عطل في منظومات الرصد لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل والنزاهة.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج العمل الأمني ضد التلاعب الممنهج بالبيانات.

اليوم الخامس :

هندسة الاستجابة الاستباقية وتصفير البيروقراطية في القيادة الأمنية وإدارة المخاطر المؤسسية

مختبر "القرار السيادي" وإدارة المخاطر الكبرى تحت الضغط

- محاكاة "الاختراق الهجين" والسيادة الرقمية: وضع القادة في سيناريو يحاكي تهديداً أمنياً مزدوجاً (سيبراني وميداني) يستهدف الأصول الحيوية، واختبار القدرة على تفعيل "بروتوكول الحصانة اللحظية" بنزاهة ووضوح تام، لضمان استمرارية الأعمال وحماية السمعة الوطنية من أي تضليل معلوماتي.
- تصفير البيروقراطية في "هندسة التدخل الأمني": تطبيق مسار قرار صفري الإجراءات لتحريك فرق الاستجابة وإعادة تخصيص الموارد الأمنية بناءً على تحليلات التوائم الرقمية، لضمان حماية المنشأة دون انتظار الموافقات الإدارية التقليدية التي قد تعيق سرعة الحماية، مع الحفاظ على الحصانة القانونية والسيادة المعلوماتية الكاملة والريادة العالمية.
- هندسة "النزاهة القيادية" في تقدير الموقف: اختبار مهارة القائد في الموازنة بين مخرجات لوحات التحكم السيادية (Sovereignty Dashboards) وبين "الحكمة البشرية القيادية" لضمان عدم حدوث انحيازات رقمية في تقدير الأخطار، وضمان استقرار جودة الحياة والتميز في الأداء الحكومي بنزاهة وشفافية مطلقة.
- ورشة "تشريح المخاطر والمقارنة الاستراتيجية": مراجعة فورية لنتائج المحاكاة لتحديد الفجوات في مصفوفة المخاطر، مع إجراء مقارنة بين النموذج الإماراتي في تصفير البيروقراطية الأمنية والنموذج الكويتي في تطوير منهجيات التدقيق، للخروج برؤية موحدة تعزز ريادة المنطقة كحصن أمن ذكي ومنيع بوضوح تام أمام المجتمع والشركاء.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة أمنية تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة 100%.
- القدرة على هندسة منظومات رصد استباقية رشيقة وسيادية تتوافق مع متطلبات الريادة والتميز العالمية.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي في النتائج.
- بناء سجل ممارسات فضلى في إدارة الذكاء الأمني الاستراتيجي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء الإدارات الأمنية والمخاطر في الجهات السيادية والحكومية.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي.
- خبراء الحوكمة والنزاهة والرقابة الداخلية المعنيون بأمن المنشآت والبيانات.
- رؤساء فرق العمل الميدانية ومحللو المخاطر الاستراتيجية في المؤسسات الوطنية.

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)