



الجمعية العمومية – الدورة الثانية والأربعون

اللجنة التنفيذية

البند رقم ١٣ من جدول الأعمال: أمن الطيران – السياسة العامة

ضرورة تعزيز دور العنصر البشري وتدابير إدارة الأمن الإلكتروني في مجال أمن الطيران

(ورقة مقدمة من كوبا بدعم من ١٧ دولة عضواً في لجنة الطيران المدني لأمريكا اللاتينية^٢)

الموجز التنفيذي

تتناول هذه الورقة العوامل البشرية وأثرها على تنمية وأداء العاملين في مجال أمن الطيران، وهو مجال أساسي يُمكن من خلاله وضع استراتيجيات واتخاذ خطوات إضافية لاستقطاب المتخصصين في أمن الطيران، وتوفير الاستقرار الوظيفي للمتدربين في هذه الوظائف بشكل عام. ويتطلب الأمر تضافر الجهود لمواصلة تعزيز أمن الطيران، وهو عنصر أساسي للتنمية المستدامة للنقل الجوي، من خلال استقطاب الكفاءات المؤهلة والمدرّبة والاحتفاظ بها لتدبير فعالية وكفاءة المنظومة وتحافظ عليهما.

الإجراءات: الجمعية العمومية مدعوة إلى:

(أ) الإحاطة علماً بالمعلومات المقدمة؛

(ب) حثّ الدول على تعزيز تدابير إدارة العوامل البشرية والأمن الإلكتروني في مجال أمن الطيران، على سبيل المثال:

- وضع خطط شاملة لإدارة العوامل البشرية والأمن الإلكتروني، بما يتماشى مع أحكام الملحق السابع عشر لاتفاقية شيكاغو واستراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران؛
- إجراء عمليات تقييم دورية للمخاطر وتحديث التدابير الوقائية؛
- تعزيز التعاون الوطني والدولي لتبادل المعلومات وأفضل الممارسات؛
- توفير التدريب المستمر للموظفين في مجال الأمن الإلكتروني والعوامل البشرية؛
- تعزيز ثقافة تنظيمية تركز على الأمن الرقمي والقدرة على الصمود.

الأهداف الاستراتيجية:	ترتبط ورقة العمل هذه بالهدف الاستراتيجي "ضمان السلامة والأمن لكل رحلة جوية"
الآثار المالية:	الموارد اللازمة لتوظيف وتدريب العاملين والاستثمار في التكنولوجيا.
المراجع:	الوثيقة Doc 10118، "الخطة العالمية لأمن الطيران" (GASep)، الطبعة الثانية القرار ٤١-١٨، "البيان الموحد بسياسات الإيكاو المستمرة المتعلقة بأمن الطيران" القرار ٤١-١٩، "معالجة الأمن الإلكتروني في مجال الطيران المدني"

^١ قدمت كوبا النسخة باللغة الإسبانية.

^٢ بليز وبوليفيا (دولة – المتعددة القوميات) والبرازيل وشيلي وكولومبيا والإكوادور والسلفادور وغواتيمالا وهندوراس وجامايكا والمكسيك ونيكاراغوا وبنما وباراغواي وبيرو وأوروغواي وفنزويلا (جمهورية – البوليفارية).

الملحق السابع عشر - "أمن الطيران" الوثيقة 8973 Doc، "دليل أمن الطيران" استراتيجية الأمن الإلكتروني في مجال الطيران إعلان مسقط بشأن أمن الطيران والأمن الإلكتروني في مجال الطيران	
---	--

١- المقدمة

١-١ يُعد أمن الطيران عنصراً أساسياً في التنمية المستدامة والفعالة للنقل الجوي في جميع أنحاء العالم. ويتطلب هذا القطاع الحيوي للترابط العالمي والنمو الاقتصادي قواعد قياسية أمنية صارمة لضمان عمليات آمنة وموثوقة. وفي هذا السياق، تؤدي العوامل البشرية دوراً حاسماً، إذ يعتمد منع الوقائع والحوادث بشكل كبير على تدريب الموظفين وأدائهم واتخاذ القرارات في جميع مراحل العمليات الجوية. وبالإضافة إلى ذلك، لا يمكن تحقيق النجاح في تطبيق القواعد القياسية والإجراءات الدولية إلا من خلال إدارة فعالة للعوامل البشرية، وهو مجال يتطلب المزيد من الدراسة والتطبيق لتعزيز الأمن وضمان قدرة منظومة الطيران على الصمود.

٢-١ وقد دفع التعقيد المتزايد للطيران، الناجم عن التطور التكنولوجي وظهور تهديدات جديدة، المجتمع الدولي إلى وضع أطر تنظيمية متينة. وفي هذا الصدد، يُعد الملحق السابع عشر الصادر عن الإيكاو هو اللائحة الأساسية لحماية الطيران المدني من أعمال التدخل غير المشروع، بما في ذلك التهديدات المادية والتهديدات الإلكترونية. ويُقرّ الملحق بأن أمن الطيران لا يقتصر على الحواجز والإجراءات المادية فحسب، بل يشمل أيضاً إدارة شاملة للعوامل البشرية والأمن الإلكتروني. وقد أصبح كلا العنصرين ضروريين لضمان قدرة الطيران على الصمود في مواجهة التحديات الحالية والمستقبلية.

٢- المناقشة

١-٢ تشمل العوامل البشرية جميع جوانب سلوك وأداء ومهارات وقيود أفراد الأمن. ويشمل ذلك الاختيار والتدريب، وإدارة التوتر والإرهاق، والتواصل، واتخاذ القرارات في المواقف الحرجة. وينبغي أن يتمتع العاملون في مجال الأمن بخلفية فنية ومهنية متينة، وشهادات متخصصة، وخبرة في إدارة مثل هذه المواقف. ويُعد التدريب المستمر أمراً ضرورياً لمواكبة التهديدات والتكنولوجيات في مجال الأمن دائمة التطور.

٢-٢ تشمل التحديات الحالية ما يلي:

- (أ) **نقص الموظفين المؤهلين:** يواجه القطاع تحديات في جذب الكفاءات المتخصصة والاحتفاظ بها، مما قد يُضعف فعالية التدابير الأمنية ويحد من قدرات الاستجابة للحوادث.
- (ب) **الإرهاق وعيب العمل المفرط:** قد يؤدي نقص الموارد البشرية إلى ساعات عمل طويلة، وإرهاق، وانخفاض الأداء، مما يزيد من خطر ارتكاب الأخطاء والمواقف الخطرة.
- (ج) **التكيف التكنولوجي:** تتطلب سرعة اعتماد التكنولوجيات الجديدة من الموظفين التكيف وتطوير مهاراتهم الرقمية لتشغيل الأنظمة المعقدة وحماية المعلومات الحساسة.
- (د) **إدارة المعلومات الحساسة:** يجب أن يكون الموظفون قادرين على التعامل مع البيانات السرية والاستجابة للوقائع الأمنية، بما في ذلك التهديدات الإلكترونية.
- (هـ) **التنوع والعمل الجماعي:** تتطلب الفرق متعددة الثقافات والمتنوعة من أجيال مختلفة مهارات قوية في مجالي التواصل والقيادة لمنع سوء الفهم وتعزيز التعاون.

٣-٢ وقد يؤدي نقص موظفي الأمن إلى ارتكاب أخطاء وتأخير في العمليات وانخفاض في القدرة على الاستجابة للوقائع. ويمكن أن يؤثر ذلك أيضاً على تنفيذ التدابير الأمنية ويزيد من عبء العمل، مما قد يؤدي إلى مواقف خطيرة. وقد يؤدي ذلك إلى زيادة المخاطر التشغيلية وعدم القدرة على تحديد التهديدات.

٤-٢ وتشمل استراتيجيات منع نقص الموارد البشرية والتخفيف من حدته ما يلي:

- أ) تخطيط الموارد البشرية؛
- ب) التوظيف والاحتفاظ بالموظفين؛
- ج) التدريب المستمر؛
- د) الدعم التكنولوجي؛
- هـ) تحسين ظروف العمل؛
- و) الإشراف والتحسين المستمر.

٥-٢ وقد طرحت البيئة الرقمية مخاطر وتحديات أمنية جديدة. ويُقرّ الملحق السابع عشر الصادر عن الإيكاو بأهمية الأمن الإلكتروني في الحماية من أعمال التدخل غير المشروع. وينبغي تزويد موظفي الأمن بما يلي للاستعداد لتحديد التهديدات الإلكترونية ومنعها والاستجابة لها:

- أ) التدريب على الأمن الإلكتروني: تدريب مُحدد بشأن الكشف عن التهديدات الرقمية وتطبيق بروتوكولات الاستجابة.
- ب) إدارة الوقائع الإلكترونية: تطوير المهارات اللازمة للاستجابة للوقائع التي قد تُهدد السلامة.
- ج) الوعي بالأمن الإلكتروني وثقافة الأمن الإلكتروني: تعزيز أفضل الممارسات والوعي بين الموظفين على جميع المستويات.

٦-٢ ويُحدد الملحق السابع عشر مُتطلبات تحديد أنظمة تكنولوجيا المعلومات والاتصالات الحيوية وتطبيق تدابير قائمة على تقييم المخاطر لحمايتها. وهذا يتطلب دمج الأمن الإلكتروني في برامج الأمن الوطني، والتعاون بين القطاعات، والرصد المُستمر للتدابير المعمول بها.

٣- الخلاصة

١-٣ يعد أمن الطيران منظومة معقدة وديناميكية، تُشكّل فيها العوامل البشرية العمود الفقري الذي يدعم فعالية جميع التدابير والإجراءات المعمول بها. وتعتمد قدرة الدول والمنظمات على توقع ومنع المخاطر والتهديدات التقليدية والناشئة، بما في ذلك التهديدات الإلكترونية، والتصدي لها بفعالية، إلى حدٍ كبير على حسن إدارة هذه العوامل.

٢-٣ ويُمثّل الأمن الإلكتروني تحدياً جديداً في إدارة العوامل البشرية. فقد وسّعت البيئة الرقمية نطاق التهديدات الأمنية. ويتعيّن أن يكون الموظفون مستعدين ليس فقط لمواجهة المخاطر المادية، ولكن لمواجهة المخاطر الإلكترونية أيضاً. ويتطلب ذلك ثقافة قوية للأمن الإلكتروني وتدريباً متخصصاً وبروتوكولات واضحة للتصدي للوقائع الرقمية. وأصبح تطبيق عناصر الأمن الإلكتروني في إدارة العوامل البشرية اليوم شرطاً أساسياً للحماية الشاملة للطيران المدني.

— انتهى —