A41-WP/421[1]
TE/161
2/8/22

**منظمة الطيران المدني الدولي**

**ورقة عمل**

# الجمعية العمومية — الدورة الحادية والأربعون

## اللجنة الفنية

**البند ٣٣ من جدول الأعمال : المسائل الأخرى المعروضة على نظر اللجنة الفنية**

## نظام إدارة أمن المعلومات المُطبَّق على خدمات الملاحة الجوية في فنزويلا

(مُقدَّمة من فنزويلا (جمهورية فنزويلا البوليفارية) بدعم من
بنما والجمهورية الدومينيكية وكوستاريكا)[2]


**الموجز التنفيذي**

الغرض من ورقة العمل هذه هو عرض موجز لما أُحرز من تقدُّم بشأن تطوير وتطبيق نظام إدارة أمن المعلومات في خدمات الملاحة الجوية، وبيان العملية وما يتعيَّن اتخاذه من خطوات تالية حسب الخطة.

**الإجراء :** الجمعية العمومية مدعوَّة إلى أن:

أ) تأخذ علما بالمعلومات المُقدَّمة في هذه الورقة؛

ب) نشر المبادرات المُتعلِّقة بتطوير تحليل المخاطر إلى جانب تطوير نظام إدارة أمن المعلومات؛

ج) دراسة إنشاء فريق فرعي لتبادل المعارف وأداء النظام والتجارب بشأن تنفيذ نظام إدارة أمن المعلومات المُطبَّق على خدمات الملاحة الجوية.


| | |
|---|---|
| الأهداف الاستراتيجية: | ترتبط ورقة العمل هذه بالهدفين الاستراتيجيين المُتعلِّقين بالسلامة وبسعة وكفاءة شبكة الملاحة الجوية. |
| الآثار المالية: | لا توجد |
| المراجع: | الملحق السابع عشر — *الأمن — حماية الطيران المدني الدولي من أفعال الدخل غير المشروع* (٤-٩-١ – ٤-٩-٢)<br>وثيقة الإيكاو Doc 10075، *القرارات السارية المفعول الصادرة عن الجمعية العمومية* (في ٦ أكتوبر ٢٠١٦) (القرار ٣٩–١٩)<br>نهج النظم الشامل (CSA) ٤٣–١٠٧ و٤٥–١٠٧<br>الخطة الوطنية لسلامة الطيران المدني (PNSAC)<br>سلسلة المنظمة الدولية لتوحيد المقاييس (ISO 27000)<br>القوانين واللوائح الفنزويلية |

[1] قدَّمت فنزويلا (جمهورية فنزويلا البوليفارية) النسخة باللغة الإسبانية.

[2] الدول الأعضاء في لجنة الطيران المدني لأمريكا اللاتينية (LACAC).

## ١ – المقدمة

١–١ عملا بتوصيات الإيكاو الواردة في الملحق السابع عشر، وباتباع الممارسات السليمة الأخرى التي أرستها سلسلة المعيار القياسي ISO 27000 فيما يتعلَّق بتنفيذ نظام إدارة أمن المعلومات وتحديثه وإدارته، فقد بدأ تقييم نظم تكنولوجيا المعلومات والاتصالات والبيانات الهامة المستخدمة في خدمات الملاحة الجوية من أجل تحديد المخاطر والتدابير التي يجب اتخاذها في ضوء الخصائص والموقع المحددين لكل منها. ومن ثم يتسنى تحديد العناصر الهامة وأماكن الثغرات، بحيث يمكن اتخاذ الإجراءات المناسبة لمنع إساءة استخدامها.

١–٢ وكجزء من تطوير نظام إدارة أمن المعلومات، تم إنشاء فرقة عمل تضم ممثلين عن كل مجال من مجالات التشغيل الفنية (الرادار، والاتصالات، والمساعدات الملاحية الراديوية، ورسائل الطيران) لتحديد أي نقاط ضعف محتملة ومناقشة أفضل الممارسات من أجل الحد منها وبالتالي تفادي الحوادث. وتحقيقا لهذه الغايات، فقد تم تبادل المعارف وعُقِدَت حلقات نقاش دراسية بشأن بناء القدرات في مجالي الشبكات والأمن الإلكتروني.

## ٢ – المناقشة

٢–١ كجانب أساسي من جوانب نظام إدارة أمن المعلومات، يمكن بناء ثقافة للأمن الإلكتروني وتكييفها مع نُظُم خدمات الملاحة الجوية بالتزامن مع تحليل المخاطر الفنية الذي لا يُجرى على أساس أعطال الأجهزة فحسب، بل أيضا على أساس الهجمات المحتملة على النظام، وذلك بسبب التحوُّل إلى التمثيل الرقمي (الرقمنة) وتكامل النُظُم والخدمات.

٢–٢ وعلاوة على ذلك، من الأهمية بمكان الاعتماد على الموارد البشرية للخدمات (الاتصالات السلكية واللاسلكية، والحاسوب، والإلكترونيات، وغيرهم من المهندسين)، الذين يجب أن يكونوا على أهبة الاستعداد لتطوير وتحسين ودراسة تدابير الأمن الإلكتروني وتكييفها مع الخدمات. ويجب على فرقة العمل إعادة تقييم العديد من سياسات السلامة لتحديد أيها الآمن منها وأيها يجب تنفيذه من أجل تحسين السياسات القائمة خطوة بخطوة.

٢–٣ وينبغي لأفرقة الخبراء أن تحدد أهمية إذكاء الوعي بشأن الأمن الإلكتروني عبر تنظيم حملات للتوعية (حلقات دراسية، ورسوم بيانية تصويرية، وما إلى ذلك) ليس للموظفين الفنيين فحسب، بل أيضا لمستخدمي النظام. فذلك سيعزز إرساء ثقافة الأمن الإلكتروني التي تضمن وعي أفرقة العمل الفنية والتشغيلية بالمخاطر الجديدة القائمة.

٢–٤ ويتمثل الهدف النهائي لتطوير نظام إدارة أمن المعلومات في تمهيد الطريق لإنشاء وحدة للأمن الإلكتروني يتولى إدارتها متخصِّصو نظام خدمات الملاحة الجوية ممن خضعوا للتدريب وبناء القدرات في هذا المجال من مجالات المعرفة. وسيقود فريق العمل التابع لهذه الوحدة الدعم والتوجيه في مسائل الأمن الإلكتروني للنظام عندما تبدأ الأنظمة في الانخراط مع الشبكات الأخرى.

٢–٥ وتتعلق إحدى الخطوات الأولى التي يجب اتخاذها بتعيين مدير لتكنولوجيا المعلومات والاتصالات يكون مُكلَّفا بتشكيل فريق العمل وجمع المعلومات اللازمة عن تطوير نظام إدارة أمن المعلومات وعن الوثائق التي يتعيَّن تقديمها. بيد أنه من المهم الإشارة إلى أن نجاح التطبيق الفعلي للنقاط المذكورة أعلاه يكمن في العمل الجماعي النشط الذي يشمل كبار مديري خدمات الملاحة الجوية، ومديري الصيانة، وأخصائيي النُظُم الفنية، ومدير مركز تكنولوجيا المعلومات.

٢–٦ يجب أن يكون عرض نظام إدارة أمن المعلومات مصحوبا بحملة توعية في مجال الأمن الإلكتروني للموظفين الفنيين والتشغيليين والإداريين لدى خدمات الملاحة الجوية

٢-٧ وثمة عامل هام آخر يلي تطوير العمليات والإجراءات، يتعلَّق بإنتاج سيناريوهات محاكاة يمكن فيها تكرار الهجمات المحتملة، مما يتيح فرصا للفنيين للتعلم والتجريب وتطبيق التدابير الأمنية اللازمة لتفادي الضرر أو الحد منه إلى أدنى قدر ممكن، مع إجراء ذلك في بيئة آمنة بمعزل عن الأنظمة.

## ٣- الخلاصة والاستنتاج

٣-١ يستلزم تطوير نظام إدارة أمن المعلومات الإقرار بالأهمية الحاسمة لكل مجال بحيث يمكن توجيه الموارد والجهود توجيها مناسبا بشكل جيد كأساس لاستمرارية الخدمة.

٣-٢ تؤدي تحليلات المخاطر إلى تحديد مواطن الضعف ليس فقط في الجوانب الفنية، بل أيضا في الجوانب التشغيلية / غير البشرية، ولهذا السبب يكتسي تنفيذها أهمية. ويمكن استخدام النتائج المتحصَّل عليها من أجل تحديد المخاطر الكامنة واتخاذ تدابير أفضل لإجراء مثل هذه التحليلات بشكل أساسي لكل خدمة أو أصل من الأصول.

٣-٣ ويعد تشكيل فريق متعدد التخصصات من المهنيين التابعين لخدمات الملاحة الجوية أمرا بالغ الأهمية لنقل المعرفة وإذكاء الوعي وتنفيذ سياسات السلامة الملائمة، مع التركيز على الحد من المخاطر إلى أدنى قدر ممكن. وعلاوة على ذلك، فسوف تؤدي حملات التوعية إلى الارتقاء بثقافة الأمن الإلكتروني، لأنها لا تؤثر في المؤسسة/الأعمال فحسب، بل تؤثر أيضا في الحياة اليومية.

٣-٤ ومن شأن تشكيل أفرقة إقليمية/دولية معنية بالأمن الإلكتروني أن تولّد الدعم والمعلومات بشأن تجارب الدول، من خلال تبادل المعلومات بشأن شراء الأجهزة، ومقدمي خدمات الأمن الإلكتروني، ومواطن الضعف التي تم تحديدها، ووسائل التوجيه. وفي ضوء التزايد اليومي للهجمات الإلكترونية، فإن هذه الأفرقة تمثل فرصة هامة للنمو في هذا المجال وتعزيز أواصر التعاون والمساعدة المتبادلة فيما بين الدول.

**— انتهى —**