Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

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

ASSEMBLÉE — 41e SESSION

COMMISSION TECHNIQUE

Point 33 : Autres questions à examiner par la Commission technique

SYSTÈME DE GESTION DE LA SÉCURITÉ DE L'INFORMATION APPLIQUÉ AUX SERVICES DE NAVIGATION AÉRIENNE AU VENEZUELA

(Note présentée par la République bolivarienne du Venezuela
et appuyée par le Costa Rica, la République dominicaine et le Panama[2])

RÉSUMÉ ANALYTIQUE

La présente note offre un survol des progrès réalisés dans l'élaboration et la mise en œuvre du système de gestion de la sécurité de l'information (ISMS) dans les services de navigation aérienne (ANS), du processus en cours et des prochaines étapes prévues.

Suite à donner : L'Assemblée est invitée à :
a) prendre note de l'information fournie dans la présente note ;
b) faire connaître les initiatives ayant trait à la préparation des analyses de risque et, simultanément, à l'élaboration d'un ISMS ;
c) envisager l'établissement d'un sous-groupe chargé de partager des connaissances ainsi que des données sur la performance des systèmes et l'expérience dans la mise en œuvre d'un ISMS appliqué aux ANS.

Objectifs stratégiques :	La présente note de travail se rapporte aux objectifs stratégiques Sécurité et Capacité et efficacité de la navigation aérienne.
Incidences financières :	
Références :	Annexe 17 – *Sûreté - Protection de l'aviation civile internationale contre les actes d'intervention illicite* (dispositions 4.9.1. et 4.9.2) Doc 10075, *Résolutions de l'Assemblée en vigueur* (au 6 octobre 2016) (résolution A39-19, pages VII-24 et 25) CSA 33-107, 43-107 et 45-107 Plan national de sécurité de l'aviation civile (PNSAC) Série ISO 27000 Lois et règlements du Venezuela

[1] Version en espagnol fournie par la République bolivarienne du Venezuela.
[2] États membres de la Commission latino-américaine de l'aviation civile (CLAC)

1. INTRODUCTION

1.1 Dans l'esprit des recommandations contenues dans l'Annexe 17 de l'OACI et d'autres bonnes pratiques établies dans la série ISO 27000 concernant la mise en œuvre, la maintenance et la gestion d'un système de gestion de la sécurité de l'information (ISMS), l'évaluation des systèmes de technologie de l'information et des communication, et des données critiques utilisées dans les services de navigation aérienne (ANS), a été menée dans le but de définir les risques et les mesures à prendre eu égard aux caractéristiques spécifiques et à l'emplacement de chaque type de risque. Cet exercice permettra de savoir quels sont les éléments critiques et où se situent les failles, de manière à prendre les mesures appropriées pour empêcher qu'elles soient exploitées.

1.2 Dans le cadre de l'élaboration du ISMS, une équipe spéciale composée de représentants de chaque secteur opérationnel (radars, communications, aides radio à la navigation et messagerie aéronautique) a été établie en vue de relever les possibles vulnérabilités et discuter des meilleures pratiques pour les atténuer afin de prévenir les incidents. Un échange de connaissances a eu lieu au sein de groupes d'étude qui se sont penchés sur la formation dans les domaines des réseaux et de la cybersécurité.

2. ANALYSE

2.1 Un aspect fondamental d'un ISMS consiste à créer une culture de cybersécurité adaptée aux systèmes des services de navigation aérienne et à perfectionner l'analyse des risques pour aller au-delà des pannes de matériel pour aborder également d'éventuelles attaques contre les systèmes, vu le degré d'informatisation et d'intégration des systèmes et des services.

2.2 Il est également très important de bien tirer parti des ressources humaines (ingénieurs en télécommunications, informatique, électronique, etc.) des différents secteurs, qui doivent s'attacher à développer, améliorer et examiner des mesures de cybersécurité adaptées aux services. L'équipe spéciale doit réévaluer bon nombre de politiques de sécurité pour déterminer à quel point elles permettent d'assurer la protection et lesquelles doivent être mises en œuvre pour améliorer graduellement les mesures en place.

2.3 Les groupes de travail devraient examiner la pertinence de mener des campagnes de sensibilisation sur la cybersécurité (rencontres, infographie, etc.), à l'intention du personnel technique mais aussi des usagers des systèmes. Le but est d'établir une culture de la cybersécurité et faire en sorte que les membres des équipes techniques et d'exploitation soient conscients des nouveaux risques.

2.4 L'objectif ultime de l'élaboration d'un ISMS est de créer les conditions pour l'établissement d'une unité chargée de la cybersécurité gérée par les spécialistes des systèmes ANS, qui auront bénéficié d'une formation et d'un renforcement des capacités en la matière. Cette équipe spéciale sera la principale source de soutien et d'orientation en ce qui concerne la sécurité des systèmes lorsque ces systèmes s'ouvriront à d'autres réseaux.

2.5 Une des premières étapes consiste à désigner un responsable des technologies de l'information et des communications (TIC) à qui il reviendra de mettre sur pied l'équipe spéciale et de recueillir l'information nécessaire pour élaborer le ISMS et les documents d'appui. Il importe néanmoins de préciser que le succès dans la réalisation des étapes énumérées ci-dessus réside dans le travail d'équipe,

où tous les membres de l'équipe --la direction des ANS, le secteur de la maintenance, les spécialistes des systèmes et le responsable des TIC-- prennent une part active aux travaux.

2.6 La présentation du ISMS doit être assortie d'une campagne de sensibilisation à la cybersécurité à l'intention du personnel technique, administratif et opérationnel des services de navigation aérienne.

2.7 Autre facteur important : une fois les procédures et mécanismes en place, il faut prévoir la tenue de simulations d'attaques éventuelles qui permettront aux techniciens d'apprendre, d'expérimenter et d'appliquer les mesures de sécurité qui s'imposent pour prévenir ou réduire au minimum les conséquences de ces atteintes. Les simulations doivent être effectuées dans un cadre sûr, et de façon isolée des systèmes.

3. CONCLUSION

3.1 L'élaboration d'un ISMS permet de relever la criticité de chaque secteur afin de cibler au mieux les ressources et les efforts pour assurer la continuité des services.

3.2 L'analyse des risques permet aussi de reconnaître les vulnérabilités, non seulement du point de vue technique, mais aussi humain et opérationnel, d'où sa pertinence. Les résultats de l'analyse servent à déterminer les risques latents et les mesures optimales pour les contrer dans chaque service ou pour les différents éléments d'actif.

3.3 La mise sur pied d'une équipe multidisciplinaire de professionnels des ANS est cruciale pour assurer le transfert des connaissances, la sensibilisation et la mise en œuvre des politiques de sécurité appropriées destinées à réduire ces risques au minimum. De plus, les campagnes de sensibilisation serviront à éduquer le personnel et à souligner le fait que la sécurité de l'information n'est pas un problème qui touche seulement l'entreprise ou l'institution, mais la vie de tous les jours.

3.4 La création de groupes régionaux et internationaux dans le domaine de la cybersécurité assurera la diffusion d'informations sur l'expérience des États et sera une source de soutien. Ces groupes échangeront des informations sur l'acquisition d'équipements, les fournisseurs de services de sécurité informatique, les vulnérabilités détectées et leur résolution, etc. Alors que les attaques évoluent au quotidien, ça sera l'occasion de progresser ensemble dans ce domaine et de renforcer la coopération et l'assistance mutuelle entre les États.

— FIN —