Organisation de l'aviation civile internationale

A41-WP/488[1]
EX/235
02/8/2022

NOTE DE TRAVAIL

ASSEMBLÉE – 41e SESSION

Point 15 : Programmes d'audits – Méthode de surveillance continue

RENFORCEMENT DES ÉQUIPES D'AUDIT USAP-CMA POUR L'ÉVALUATION ET LA MISE EN ŒUVRE DES EXIGENCES DE L'ANNEXE 17 EN MATIÈRE DE CYBERSÉCURITÉ

(Note présentée par la République bolivarienne du Venezuela et appuyée par la Bolivie (État plurinational de), la Colombie, le Costa Rica, le Panama, le Pérou et l'Uruguay)[2]

RÉSUMÉ ANALYTIQUE

Dans le cadre du Programme universel d'audits de sûreté (USAP), les États disposent actuellement de lignes directrices qui permettent une évaluation générale des performances du système de supervision de la sûreté de l'aviation nationale. Il est ainsi possible d'élaborer des recommandations d'amélioration à partir de principes communs de sûreté de l'aviation. Cette évaluation est menée par une équipe d'auditeurs qui s'assure que ces activités couvrent les éléments essentiels du système de supervision de la sûreté de l'aviation, en plus des dispositions et du niveau de conformité aux normes de l'Annexe 17 - *Sûreté de l'aviation*. L'Annexe 17 indique comment élaborer et mettre en œuvre des mesures de protection des systèmes de technologies de l'information et des communications, ainsi que des données critiques utilisées dans l'aviation civile. Dans cette optique, il est nécessaire de renforcer les équipes d'audit par l'élaboration d'éléments indicatifs et de supports de formation qui leur permettront d'évaluer et de mettre en œuvre les exigences de cybersécurité énoncées à l'Annexe 17.

Suite à donner : L'Assemblée est invitée à :
a) prendre note des informations présentées dans la présente note de travail ;
b) demander au Conseil de développer des outils ou du matériel de formation pour fournir à l'équipe d'audit de l'USAP des orientations et une formation complètes en matière de cybersécurité, afin que les groupes désignés puissent procéder à une évaluation objective et technique des questions de protocole (PQ), conformément aux aspects de la cybersécurité particuliers à l'aviation civile.

Objectifs stratégiques :	La présente note de travail se rapporte à l'objectif stratégique : Sûreté et facilitation.
Incidences financières :	Nous proposons que les activités mentionnées dans ce document soient entreprises sous réserve de la disponibilité de ressources dans le budget-programme ordinaire du triennat actuel et/ou de contributions extrabudgétaires.
Références :	Pratique recommandée 4.9.1 de l'Annexe 17 et Protocole USAP-CMA.

[1] Version espagnole fournie par la République bolivarienne du Venezuela.
[2] États membres de la région Amérique du Sud (SAM) et de la Commission latino-américaine de l'aviation civile (LACAC).

1. INTRODUCTION

1.1 Le Programme universel d'audits de sûreté (USAP) fournit aux États des lignes directrices qui permettent une évaluation générale des performances du système de supervision de la sûreté de l'aviation de l'État. Il est ainsi possible d'élaborer des recommandations d'amélioration à partir de principes communs de sûreté aérienne. Selon la méthode de surveillance continue de l'USAP (USAP-CMA), il existe actuellement des PQ spécifiques (1345, 1350, 1360 et 3278) pour l'évaluation des aspects généraux ou fondamentaux de l'élaboration et de la mise en œuvre de mesures de protection des systèmes de technologies de l'information et des communications, ainsi que des données critiques utilisées dans le cadre de l'aviation civile.

1.2 Cette évaluation est menée par une équipe d'auditeurs USAP qui s'assure que ces activités couvrent les éléments essentiels du système de supervision de la sûreté de l'aviation, ainsi que les dispositions des et le niveau de conformité aux normes de l'Annexe 17 - *Sûreté de l'viation*. L'Annexe 17 comprend l'engagement de chaque État à attribuer des responsabilités, à établir des critères nationaux de protection des systèmes associés à l'exploitation aérienne par la mise en œuvre de mesures de protection, à identifier les systèmes critiques, à assurer une surveillance continue, à garantir la détection, l'analyse et la réaction aux cyberattaques et à évaluer les activités de contrôle de la qualité menées par l'État conformément aux évaluations des risques.

2. ANALYSE

2.1 Compte tenu de l'importance des activités menées dans le cadre de l'USAP-CMA, il est important, dans le domaine de la cybersécurité, de veiller à ce que l'équipe en charge des audits USAP dispose d'éléments indicatifs qui lui permettent de procéder à une évaluation objective et technique de la mise en œuvre des normes, stratégies et meilleures pratiques internationales élaborées et appliquées par les États afin d'identifier et de protéger les systèmes critiques de technologie de l'information et des communications contre toute interférence susceptible de compromettre la sécurité, l'intégrité ou le fonctionnement du système de l'aviation civile.

2.2 Nous disposons actuellement de cadres de référence et de pratiques existantes au niveau mondial qui ont permis à diverses organisations de gérer efficacement et de réduire les risques de cybersécurité. À titre d'exemple, citons les normes de la série ISO/IEC-2700 conçues pour établir de bonnes pratiques relativement à divers aspects de la gestion de la sécurité de l'information, de l'amélioration continue et de l'atténuation des risques ; le guide des objectifs de contrôle de l'information et des technologies associées (COBIT) ; la méthodologie d'analyse et de gestion des risques pour les systèmes d'information MAGERIT ; d'autres normes, lignes directrices et meilleures pratiques internationales.

2.3 Les documents de référence susmentionnés constituent un progrès significatif en matière de coopération et d'intégration mondiale dans le domaine de la cybersécurité en fournissant des lignes d'action et des critères de référence applicables et communs à tous les types d'infrastructures critiques. Ces références portent spécifiquement sur les normes, lignes directrices et pratiques de l'industrie qui rendent possibles la mise en œuvre et les évaluations de la cybersécurité, non seulement au niveau de l'organisation et de la documentation, mais aussi en ce qui concerne les opérations et la mise en œuvre.

2.4 Dans cette optique, nous proposons l'élaboration d'éléments indicatifs normalisés afin de permettre la création d'un cadre de référence fondé sur les meilleures pratiques et méthodologies de l'industrie et l'expérience des États afin de déterminer une approche harmonisée. Il n'est pas nécessaire d'élaborer un document statique : des éléments indicatifs permettraient à l'équipe d'auditeurs USAP de

fournir une évaluation technique et objective du niveau de la conformité aux normes sur la base des spécificités et des besoins de chaque État, comme présentés dans les PQ 1345, 1350, 1355, 1360 et 3278.

2.5 L'appendice de la présente note de travail suggère un modèle de contenu pour les domaines de connaissance et les éléments indicatifs. La proposition se fonde sur des critères tirés de diverses normes, lignes directrices et pratiques existantes en matière de gestion de la sécurité de l'information, d'amélioration continue et d'atténuation utilisées dans des organisations disposant d'infrastructures critiques au niveau international. L'Appendice met en évidence les points suivants :

a) les domaines de connaissance et l'expérience potentiellement nécessaires à l'évaluation des mesures de cybersécurité mises en œuvre par les États (selon les PQ) ;

b) le contenu suggéré pour la rédaction d'un texte ou d'éléments indicatifs permettant à l'équipe d'audit USAP d'évaluer et de mettre en œuvre les exigences de cybersécurité énoncées à l'Annexe 17.

3. CONCLUSION

3.1 Il est essentiel que les équipes d'audit affectées à la mise en œuvre de l'USAP-CMA possèdent les outils et les connaissances nécessaires à une évaluation précise et objective du respect par l'État de la conception, de l'élaboration et de la mise en œuvre de tâches de protection de la cybersécurité pour l'aviation civile, conformément aux exigences énoncées dans les normes et pratiques recommandées de l'Annexe 17 de l'OACI – *Sûreté de l'aviation*.

— — — — — — — —

APPENDICE

CONTENU SUGGÉRÉ EN MATIÈRE DE DOMAINES DE CONNAISSANCE ET D'ÉLÉMENTS INDICATIFS

a) Domaines de connaissance et d'expérience nécessaires à l'évaluation des mesures de cybersécurité mises en œuvre par les États

Connaissance des procédures et des techniques de gestion des ressources et des processus critiques ; identification et évaluation des ressources technologiques ou informations associées à l'aviation ; politiques, procédures et mesures de sécurité de l'information ; gestion des risques et des incidents ; contrôles de gestion ou mécanismes de protection permettant d'atténuer les problèmes de cybersécurité découverts ; audits judiciaires, de réseau, de code, de vulnérabilités et physiques, analyse web, etc.

Capacité technique d'évaluer les mesures de protection par le biais de tests : collecte, classification et identification des ressources, analyse des services, analyse et validation de vulnérabilité ; contrôles d'essais opérationnels du système d'alimentation électrique, des équipements, des ressources ou systèmes dépendants en cas de panne du système électrique ; test d'équipements de gestion des systèmes et plates-formes informatiques ; tests de matériel, de logiciels d'exploitation et d'infrastructure et/ou d'applications logicielles ; tests de performance de la plate-forme informatique (en conditions d'interruption totale) ; test du service de sauvegarde Internet (déconnexion du canal primaire, vérification de la connexion du canal secondaire, équilibrage de la charge, etc.) ; tests de récupération de l'information, et autres.

b) Contenu suggéré pour la rédaction d'un texte ou d'éléments indicatifs permettant l'évaluation et la mise en œuvre des exigences en matière de cybersécurité énoncées à l'Annexe 17.

1. Guide des processus critiques communs dans l'industrie de l'aviation civile pour ce qui concerne les compagnies aériennes (gestion des passagers, des bagages et du fret, assistance au sol, régulation des vols, maintenance des avions, entre autres) ; processus critiques dans les aéroports (sécurité, exploitation et infrastructures aéroportuaires, gestion et urgences aéroportuaires, entre autres) ; processus critiques de gestion du transport aérien (communications vocales, messagerie aéronautique et données radar, navigation aérienne, entre autres).

2. Méthodologie normalisée d'évaluation des risques pour le secteur de l'aviation qui inclut la détermination du contexte, des politiques et des responsabilités, l'identification des processus opérationnels, l'identification et l'évaluation des ressources, l'identification des vulnérabilités et l'identification des menaces, leur probabilité d'occurrence et leur impact estimé (conséquences).

3. Orientations relatives aux contrôles ou mécanismes de protection, y compris la gestion du matériel réseau, la gestion des logiciels autorisés et non autorisés, la configuration de base des appareils mobiles, ordinateurs portables, ordinateurs de bureau et serveurs, le processus continu d'identification et de correction des vulnérabilités, les processus et outils d'identification, de prévention et de correction de l'utilisation et de la configuration des privilèges administratifs (réseaux/applications), la maintenance, le suivi et l'analyse des résultats d'audit, les procédures de protection du courrier électronique et des navigateurs, la gestion des ports, des protocoles et des services dans les appareils du réseau ; des procédures basées sur des méthodologies et outils appropriés pour la sauvegarde des informations critiques et les tests de récupération ; des procédures de configuration sécurisée des dispositifs de réseau (pare-feu, routeurs et commutateurs), défense du périmètre ; des procédures et outils de protection des données pour prévenir la perte d'informations, atténuer les incidents et garantir la confidentialité et l'intégrité des informations sensibles ; des procédures de gestion et de réponse aux incidents et d'autres contrôles.

— FIN —