Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

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

ASAMBLEA — 41º PERÍODO DE SESIONES

COMISIÓN TÉCNICA

Cuestión 33: Otros asuntos que habrá de considerar la Comisión Técnica

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADA A LOS SERVICIOS A LA NAVEGACIÓN AÉREA EN VENEZUELA

[Nota presentada por Venezuela (República Bolivariana de) y apoyada por Costa Rica, Panamá y República Dominicana][2]

RESUMEN

Esta nota de estudio tiene por finalidad presentar un resumen de los avances en el desarrollo y aplicación del Sistema de Gestión de Seguridad de la Información (SGSI) en los Servicios a la Navegación Aérea (SNA), proceso y los próximos pasos previstos.

Decisión de la Asamblea: Se invita a la Asamblea a:
a) tomar nota de la información proporcionada;
b) difundir las iniciativas en el desarrollo de los análisis de riesgo y con ello el desarrollo del SGSI, y
c) estudiar la creación de un Sub Grupo, a través de los cuales se comparta saberes, comportamiento de sistemas y experiencias en la implementación del SGSI aplicados a los SNA.

Objetivos Estratégicos:	Esta nota de estudio se relaciona con los Objetivos estratégicos de seguridad operacional y Capacidad y eficiencia de la navegación aérea
Repercusiones Financieras:	
Referencias:	*Anexo 17 — Seguridad de la aviación – Protección de la aviación civil internacional contra los actos de interferencia ilícita* (4.9.1 - 4.9.2) *Resoluciones vigentes de la Asamblea* (al 6 de octubre de 2016) (Doc 10075) (cuestión A39-19, pág. 91 a 93) CSA 43-107 y 45-107 Plan Nacional de Seguridad de la Aviación Civil (PNSAC). Serie ISO 27000. Leyes y Normativas Venezolanas

[1] Versión en español proporcionada por Venezuela (República Bolivariana de).
[2] Estados miembros de la Comisión Latinoamericana de Aviación Civil (CLAC).

1. INTRODUCCIÓN

1.1 Siguiendo las recomendaciones de la OACI en el Anexo 17 y de la mano con otras buenas prácticas establecidas en la serie ISO 27000 para la implementación, mantenimiento y gestión del "Sistema de Gestión de Seguridad de la Información", se da inicio a la evaluación de los sistemas de tecnología de la información de las comunicaciones y datos críticos que se empleen en los SNA, para así determinar los riesgos y las medidas que deben ser implementadas, tomando en cuenta la particularidad de cada uno y su ubicación. Gracias a ello se logra saber cuáles son los elementos críticos y en dónde tenemos una brecha, permitiendo tomar acciones adecuadas para evitar que las mismas sean explotadas.

1.2 El desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI) ha permitido conformar un equipo de trabajo integrado por representantes de cada área técnica operativa (Radar, Comunicaciones, Radioayudas y Mensajería Aeronáutica), creado con el objetivo del reconocimiento de las posibles vulnerabilidades y discusión de las mejores prácticas para reducirlas y con ello evitar incidentes. Esto a través del intercambio de conocimientos y mesas de estudio, donde se contempla la capacitación en el área de redes y ciberseguridad.

2. ANÁLISIS

2.1 Como aspecto fundamental para un SGSI de debe establecer una cultura de ciberseguridad adaptada a los sistemas de los Servicios a la Navegación Aérea, y a su vez evolucionar los análisis de riesgos técnicos no solamente basándose en las posibles fallas de los equipos, sino también a los posibles ataques que puedan ser víctima los sistemas, considerando la digitalización e integración de los sistemas y servicios.

2.2 Igualmente es de gran importancia el aprovechamiento del recurso humano (Ingenieros en Telecomunicaciones, Informáticos, Electrónicos, etc.) perteneciente a los servicios, los cuales deben estar dispuestos a desarrollar, mejorar y estudiar medidas de ciberseguridad ajustadas a los servicios. Estos equipos de trabajo deben reevaluar muchas políticas de seguridad en donde se determinan que tan seguras son y cuáles deberían ser implementadas para ir mejorando paso a paso las existentes.

2.3 A través de las mesas de trabajo se debería determinar la importancia de implementar campañas de concientización de ciberseguridad (charlas, infografías, etc.), no únicamente para el personal técnico, sino también a los usuarios de los sistemas. Con esto se persigue establecer una cultura de ciberseguridad que nos permitirá contar con un equipo de trabajo técnico y operativo consciente de los nuevos riesgos existentes.

2.4 El objetivo final del desarrollo de un SGSI es ir preparándonos para la creación de una dependencia de ciberseguridad administrada por especialistas de los sistemas de SNA, los cuales sean formados y capacitados en dicha área del saber. En donde ese equipo de trabajo sea nuestro principal apoyo y guía en lo que se refiere a la ciberseguridad para los sistemas, cuando los sistemas comiencen a tener puertas abiertas a otras redes.

2.5 Una de las primeras acciones a tomar debe ser la designación de un responsable en Tecnología de la Información y Comunicaciones (TIC), encargado de conformar el equipo de trabajo y recaudar la información necesaria para el desarrollo del SGSI y los documentos que deban ser realizados; sin embargo, es importante acotar que el éxito de la aplicabilidad real de los ítems mencionados anteriormente está en el trabajo de equipo, donde se involucran activamente; la alta gerencia del SNA, la gerencia de mantenimiento, los técnicos especialistas de los sistemas y el responsable TIC.

2.6 La presentación del SGSI, debe estar acompañada con la campaña de ciberseguridad para el personal técnico, operativo y administrativo de los Servicios a la Navegación Aérea.

2.7 Otro factor importante, es que después de establecidos los procesos y procedimientos se debe prever la creación de escenarios simulados dónde se puedan recrear los posibles ataques, lo que permitirá dar la oportunidad a los técnicos de aprender, experimentar y aplicar las medidas de seguridad necesarias para evitar o minimizar la afectación, estos serán desarrollados bajo un ambiente seguro y aislado de los sistemas.

3. CONCLUSIÓN

3.1 El desarrollo de un SGSI permite reconocer la criticidad de cada área, con ello poder enfocar los recursos y esfuerzos de manera adecuada y bien direccionada en base a la continuidad de los servicios.

3.2 Los análisis de riesgos permiten que reconocer las vulnerabilidades que se tienen no solo en el área técnica sino también en el área humana/operacional, es por ello que se considera relevante su ejecución. Con esos resultados se podrá determinar el riesgo latente y las mejores medidas para aplicarlo en base a cada servicio o activo.

3.3 La conformación de un grupo multidisciplinario de profesionales de los SNA, es fundamental para la transferencia de conocimientos, concientización e implementación de las políticas de seguridad adecuadas, enfocadas a minimizar los riesgos. Adicionalmente, las campañas de concientización permitirán crear una educación de ciberseguridad, puntualizando que la afectación no sólo es a nivel de Institución/Empresa sino en la vida cotidiana.

3.4 La creación de grupos regionales/internacionales en esta área de ciberseguridad, permitirá contar con apoyo e información sobre las experiencias de los Estados. Intercambiando información de adquisición de equipos, proveedores de servicios en ciberseguridad, vulnerabilidades detectadas y cómo fueron canalizadas, ya que los ataques de ciberseguridad evolucionan diariamente. Se considera una oportunidad importante para crecer en esta área y fortalecer los lazos de cooperación y ayuda mutua entre los Estados.

— FIN —