Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

A41-WP/231[1]
EX/104
2/8/22

ASAMBLEA — 41º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Cuestión 14: Seguridad de la aviación — Política

ESTRATEGIA DE CULTURA DE LA CIBERSEGURIDAD

[Nota presentada por Arabia Saudita en nombre de los Estados de la Organización Árabe de la Aviación Civil (OAAC)[2]]

RESUMEN

Los ciberataques no dejan de aumentar en el sector de la aviación civil, lo que a su vez repercute en los aeródromos, las compañías aéreas, el tráfico aéreo y el público usuario. El mejor método para minimizar los riesgos es formular una estrategia para establecer una cultura de la ciberseguridad orientada a acrecentar la capacidad del personal, promocionar los objetivos de ciberseguridad y proteger a las organizaciones frente a las ciberamenazas internas y externas. La estrategia de la cultura de la ciberseguridad está destinada a desempeñar un papel fundamental para cumplir los requerimientos de ciberseguridad y propiciar la cooperación en las organizaciones y también a escala nacional e internacional. La estrategia debe dirigirse a todo el personal de la organización, ya que su objetivo es establecer y mantener una cultura de la ciberseguridad que beneficie a la gente, las tecnologías y las operaciones de ciberseguridad.

Medidas propuestas al Comité: Se invita a la Asamblea a:

a) instar a los Estados miembros a que adopten una estrategia de cultura de la ciberseguridad en la aviación civil frente a la multiplicación de los ciberataques en todo el mundo; y
b) pedir a la OACI que desarrolle un programa de concientización en ciberseguridad destinado al personal de la aviación civil, en paralelo al programa de Cultura de la Seguridad de la Aviación.

Objetivos estratégicos:	Esta nota de estudio se relaciona con el objetivo estratégico de *Seguridad de la aviación y facilitación*.
Repercusiones financieras:	
Referencias:	

[1] Versión en árabe proporcionada por Arabia Saudita.

[2] Estados miembros de la Organización Árabe de la Aviación Civil (OAACI: Arabia Saudita, Argelia, Bahrein, Comoras, Djibouti, Egipto, Emiratos Árabes Unidos, Iraq, Jordania, Kuwait, Líbano, Libia, Marruecos, Mauritania, Omán, Palestina, Qatar, Somalia, Sudán, República Árabe Siria, Túnez y Yemen.

1. INTRODUCCIÓN

1.1 El error humano ha sido citado como la causa principal de ataques y vulneraciones de ciberseguridad en 2021, lo que sugiere que el personal es el eslabón más débil de la cadena de ciberseguridad. Además, el ciberdelito ha orquestado ataques dirigidos a las usuarias y los usuarios del sistema para explotar sus vulnerabilidades. Frente a esta situación, las organizaciones deben desarrollar estrategias para establecer una cultura de la ciberseguridad a fin de que el personal sepa responder ante la gran variedad de ciberamenazas dirigidas a su persona o al puesto que ocupan. De esta forma, el personal se convierte en la primera línea de defensa de la organización.

1.2 Las personas, los procesos y las tecnologías constituyen los tres pilares principales de la ciberseguridad. Los tres pilares dependen de manera crucial de la existencia de una sólida cultura de la ciberseguridad, ya que sin personal correctamente entrenado la tecnología puede crear vulnerabilidades. Los procesos en sí mismos tampoco son eficaces si el personal no los aplica correctamente.

1.3 El error humano no se limita a que las personas usuarias hagan clic en enlaces sospechosos o descarguen programas maliciosos. El riesgo más grave proviene de los errores que puede cometer una persona sin las condiciones necesarias al configurar o poner en marcha un sistema crítico o al no seguir los procedimientos de gestión del cambio al introducir modificaciones en un sistema, exponiendo así la infraestructura técnica general a ciberamenazas externas.

1.4 Todo el personal debe ser consciente de sus funciones y responsabilidades en la ejecución del programa de ciberseguridad de la organización. También debe comprender sus obligaciones en virtud de la política de ciberseguridad y del código penal nacional que rija las actividades cibernéticas.

1.5 La alta dirección y el consejo de administración desempeñan un papel crucial a la hora de promover el cumplimiento de los requisitos de ciberseguridad y dar respuesta a los riesgos. Por ello, deben ser conscientes de la importancia de la ciberseguridad y considerar que los riesgos afectan a toda la organización.

2. CULTURA DE LA CIBERSEGURIDAD

2.1 Una cultura de la ciberseguridad promueve el intercambio de información entre los Estados miembros para detectar y resolver proactivamente las ciberamenazas y vulnerabilidades.

2.2 El cambio efectivo comienza con la sensibilización y la formación en ciberseguridad, lo que significa que las organizaciones deben ir más allá y modificar el comportamiento mediante la adopción de una cultura de la ciberseguridad.

2.3 La cultura de la ciberseguridad comprende tres pasos:

a) *Definir los objetivos estratégicos:* El primer paso del proceso es fijar los objetivos de la cultura de la ciberseguridad. Dichos objetivos pueden incluir, entre otros, cerciorarse de que el personal comprenda bien los riesgos de ciberseguridad para la organización y sea consciente de las funciones y responsabilidades que le competen y mejorar los conocimientos y las competencias en ciberseguridad;

b) *Evaluar la situación existente*: El objetivo es evaluar la cultura existente, tanto a nivel individual como en toda la organización. A nivel de la organización, se refiere a la gobernanza y la promoción de las conductas correctas. Podrá incluir políticas y procedimientos, política de uso aceptable, funciones y responsabilidades, sensibilización

y formación, estructura organizacional, estructuras de ciberseguridad, notificación de incidentes y documentación del comité de ciberseguridad. Por su parte, a nivel individual evalúa la conciencia del personal en materia de ciberseguridad a través de plataformas de aprendizaje o simulaciones de ciberataques. Si no se dispone de las tecnologías necesarias, se puede elaborar y distribuir una encuesta para recabar la información necesaria; y

c) *Desarrollar el programa:* El último paso consiste en graficar la brecha entre la situación actual y la deseada y definir el programa para alcanzar los objetivos estratégicos fijados inicialmente.

— FIN —