Control aéreo, bajo austeridad republicana

Aunque especialistas advierten que un ciberataque contra los sistemas de control de tránsito aéreo podría tener efectos catastróficos, el Seneam reporta que durante este 2023 careció de recursos presupuestales encaminados al fortalecimiento de la ciberseguridad

Control aéreo, bajo austeridad republicana

#Ciberseguridad

Aunque especialistas advierten que un ciberataque contra los sistemas de control de tránsito aéreo podría tener efectos catastróficos, el organismo denominado Servicios a la Navegación en el Espacio Aéreo Mexicano (Seneam) reporta que durante este 2023 careció de recursos presupuestales encaminados al fortalecimiento de la ciberseguridad

POR LUIS HERRERA
@Luis_Herrera_A

El organismo denominado Servicios a la Navegación en el Espacio Aéreo Mexicano (Seneam), responsable del Control de Tránsito Aéreo en el país, careció durante este año de recursos para fortalecer sus esquemas de ciberseguridad, aun teniendo en sus manos funciones tan relevantes como la ya señalada para garantizar el transporte seguro de las personas.

Especialistas en el ámbito de la seguridad de la aviación civil han advertido que un ciberataque que logre vulnerar los sistemas de control de tránsito aéreo de un país, podría tener consecuencias muy graves, incluyendo la colisión de aeronaves en vuelo, con las pérdidas de vidas humanas que ello podría implicar.

En respuesta a una solicitud de información, donde se le requirió que precisara qué medidas había adoptado para protegerse de los ciberataques, el organismo Seneam brindó un reporte al respecto.

"En reunión virtual el 15 de diciembre de 2022, con el encargado de la implementación del Marco de Gestión de la Información, en las dependencias gubernamentales, de la Coordinación de Estrategia Digital Nacional (CEDN), se le comentó que no se cuenta con recursos financieros para la adquisición de herramientas para el fortalecimiento de la ciberseguridad, a lo cual sugirió, nos enfoquemos en la implementación de políticas, procedimientos, campañas de concientización y cuando sea posible el uso de herramientas de software libre, derivado de la austeridad republicana".

No obstante, el organismo asegura que la infraestructura de red con la cual despliega sus funciones sustantivas en materia de navegación aérea se encuentra "aislada", lo que la vuelve inalcanzable de algún ciberataque, según lo expone en el documento (recurso de revisión RRA 4264/23).

"En cuanto a las redes de misión crítica, donde se encuentran las TICs operativas para los servicios de ayuda a la navegación aérea, Servicios a la Navegación en el Espacio Aéreo Mexicano tiene una infraestructura de red que no es pública y se mantiene aislada, por lo que no es susceptible de ataques cibernéticos externos. A la fecha, no se cuenta con información que nos indique de la existencia de ataques cibernéticos y no se ha visto comprometida la seguridad y los servicios a la navegación aérea".

Para el resto de sus actividades, el organismo indica que emplea una infraestructura de red de la cual no es el administrador sino sólo un usuario.

"La infraestructura de red que utiliza Servicios a la Navegación en el Espacio Aéreo Mexicano para los servicios de Tecnologías de la Información y Comunicaciones (TICs), utilizadas para la administración (TICs Informáticas) a través de los servicios de correo institucional, internet e intranet, dicha red es propiedad de la Secretaría de Infraestructura de Comunicaciones y Transportes".

Por tal motivo, agrega que no se tiene información relacionada con ciberataques, si bien ocurrió un ataque de ciberseguridad en la Secretaría de Infraestructura de Comunicaciones y Transportes, la misma aplicó los protocolos de ciberseguridad y Servicios a la Navegación en el Espacio Aéreo Mexicano permaneció aislado de dicho ataque y no se vio comprometida la infraestructura.

Los riesgos

Este 11 de agosto de 2023, Eduardo Reyes López, subgerente de Seguridad Aeroportuaria del Grupo Aeroportuario del Pacífico (GAP), publicó un artículo en el portal de Seguritlatam, titulado Seguridad integral: ciberseguridad y AVSEC, un enfoque holístico, donde advierte sobre las consecuencias que podría tener un ciberataque en el control de tránsito aéreo.

"El gran secreto de la integración de la ciberseguridad en el ambiente AVSEC (Seguridad de la Aviación Civil) es estar conscientes de cuánto depende la vida de las personas (pasajeros, tripulaciones, comunidad del aeropuerto y población en general) de las computadoras o sistemas informáticos, así como de la vulnerabilidad de los mismos. Si somos capaces de identificar esto, el camino, sin duda, será mucho más fácil".

Reyes López señala que un ciberataque de tipo ransomware, que bloquea el acceso a los sistemas de información a cambio de un rescate económico, podría tener secuelas mortales.

"En un entorno AVSEC, un ciberataque de ransomware podría ser catastrófico si, como moneda de cambio por la liberación de presos políticos (generalmente esta es una demanda de grupos terroristas), la información de los sistemas de control de tránsito aéreo fuera adulterada de tal manera que se pudieran ocasionar impactos entre aeronaves en vuelo".

Los avances

Aunque el organismo Seneam reconoce la falta de recursos para incrementar su ciberseguridad, también asegura que sí está implementando acciones en este rubro, inclusive bajo la supervisión de la Organización de Aviación Civil Internacional (OACI).

"Dentro del ámbito aeronáutico Servicios a la Navegación en el Espacio Aéreo Mexicano, como proveedor de los servicios aeronáuticos (ANSP por sus siglas en inglés) del Estado Mexicano, miembro de la Organización Internacional de Aviación Civil, se encuentra desarrollando los mecanismos de seguridad en la aviación (AVSEC) y Ciberseguridad para una navegación segura. Tales medidas también son auditadas por la OACI a través de la autoridad aeronáutica en nuestro país, la Agencia Federal de Aviación Civil".

También expone que, dado que está atendiendo los objetivos estratégicos de la OACI, dentro del Plan Global de Navegación Aérea, que persiguen una interoperabilidad de los sistemas entre ANSP para un manejo automatizado, eficiente y seguro de las operaciones aéreas, el Seneam ha iniciado un programa de modernización de sus sistemas y equipos de ayuda a la navegación aérea, los cuales ya incluyen los mecanismos de ciberseguridad en hardware y software.

Asimismo, Seneam trabaja en la implementación de su Marco de Gestión de Seguridad de la Información (MGSI), que incluye el establecimiento de una Política de Seguridad de la Información, y controles para tener un protocolo de actuación ante intervenciones ilícitas, internas o externas, que puedan causar la pérdida total o parcial de los activos de negocio de la institución.

Aunque el Seneam reconoce la falta de recursos para incrementar su ciberseguridad, también asegura que sí está implementando acciones en este rubro, inclusive bajo la supervisión de la Organización de Aviación Civil Internacional

Especialistas en el ámbito de la seguridad de la aviación civil, han advertido que un ciberataque que logre vulnerar los sistemas de control de tránsito aéreo de un país, podría tener consecuencias muy graves, incluyendo la colisión de aeronaves

"En reunión con el encargado de la implementación del Marco de Gestión de la Información de la Coordinación de Estrategia Digital Nacional, se le comentó que no se cuenta con recursos financieros para la adquisición de herramientas para el fortalecimiento de la ciberseguridad, a lo cual sugirió, nos enfoquemos en la implementación de políticas, procedimientos, campañas de concientización y cuando sea posible el uso de herramientas de software libre, derivado de la austeridad republicana"

Servicios a la Navegación en el Espacio Aéreo Mexicano (Seneam)