Organización de Aviación Civil Internacional
Grupo Regional de Planificación y Ejecución CAR/SAM (GREPECAS)
Decimoctava Reunión del Grupo Regional de Planificación y Ejecución CAR/SAM (GREPECAS/18)
Punta Cana, República Dominicana, 9 al 14 de abril de 2018

Cuestión 3 del Orden del Día: **Actividades de navegación aérea a nivel global, inter e intrarregionales**

3.2 Seguimiento en la implantación de las actividades a nivel global, inter e intrarregional

Promoción de la resiliencia cibernética a través de la concientización global y simulacros regionales

(Presentada por Estados Unidos)

RESUMEN

De conformidad con la Resolución A39-19 de la Asamblea de la OACI, la FAA está trabajando con socios dentro del ámbito de la OACI y con socios regionales para identificar las amenazas y los riesgos de posibles incidentes de ciberseguridad en las operaciones y sistemas críticos de la aviación civil, y para fomentar una interpretación común de las ciberamenazas, los riesgos y la mitigación de los incidentes cibernéticos entre los socios.

La FAA está proponiendo un modelo de simulacros de ciberseguridad, utilizando la discusión dirigida de escenarios, que permita un intercambio abierto de ideas sobre diversos temas referidos a un incidente de ciberseguridad hipotético y simulado. Este ejercicio puede ser utilizado para mejorar la conciencia general, validar los planes y procedimientos actuales, y evaluar los sistemas y actividades para la respuesta y recuperación de incidentes de ciberseguridad. Las acciones sugeridas aparecen en el párrafo 4.

Referencias:

- Resolución A39-18 de la Asamblea: Declaración consolidada de los criterios permanentes de la OACI relacionados con la seguridad de la aviación
- Resolución A39-19 de la Asamblea: Formas de abordar la ciberseguridad en la aviación civil

1. Introducción

1.1 El público viajero, la industria aeronáutica, los proveedores de servicios de navegación aérea (ANSP) y las autoridades de aviación civil (AAC) dependen cada vez más de las comunicaciones y de las operaciones basadas en redes, por lo que los Estados deben esforzarse para modernizar la infraestructura informática y de red, conectando a los usuarios, los sistemas y los datos para brindar un acceso transparente y seguro, protegido de los incidentes de ciberseguridad.

1.2 Los incidentes cibernéticos pueden afectar a la comunidad aeronáutica mundial o a los sistemas individuales en muchos niveles. Estos incidentes pueden poner en peligro las comunicaciones y los intercambios de información entre las diversas partes involucradas de la aviación, afectando la seguridad operacional y la seguridad de la aviación, y perjudicando la continuidad del negocio aeronáutico. La capacidad de compartir información cibernética y la aplicación de sólidos métodos normalizados para asegurar el intercambio de datos e información, mejoran la capacidad de la comunidad aeronáutica de auto-protegerse y limitar el impacto de los incidentes de ciberseguridad.

1.3 A fin de fortalecer la posición de la seguridad de la aviación civil, la FAA está emprendiendo la tarea de identificar los riesgos de ciberseguridad a través del ecosistema aeronáutico que pudieran afectar la seguridad operacional y alterar las operaciones del Sistema Nacional del Espacio Aéreo (NAS), y luego desarrollar estrategias de mitigación. Esta estrategia transversal permite que los componentes del NAS trabajen en conjunto como un solo sistema para garantizar la provisión de servicios seguros y eficientes al público viajero, líneas aéreas, fuerzas armadas de Estados Unidos, aviación general y aeropuertos.

1.4 Más allá del ámbito de las estrategias nacionales de mitigación de ciberseguridad y de conformidad con la Resolución A39-19 de la Asamblea de la OACI, la FAA está trabajando con sus socios en la OACI y con los socios regionales para identificar las amenazas y los riesgos de posibles incidentes de ciberseguridad en las operaciones y sistemas críticos de la aviación civil, y para fomentar una interpretación común entre los socios con respecto a las ciberamenazas y riesgos y la mitigación de los incidentes de ciberseguridad.

1.5 La FAA está proponiendo un modelo de simulacros cibernéticos a nivel regional, utilizando la discusión dirigida de escenarios, que permita un intercambio abierto de ideas sobre diversos temas referidos a un incidente de ciberseguridad hipotético simulado. Este ejercicio puede ser utilizado para mejorar la conciencia general, validar los planes y procedimientos existentes, y evaluar los sistemas y actividades para la respuesta y recuperación de incidentes cibernéticos.

Discusión

1.6 La 39ª Asamblea de la OACI, a través de la Resolución A39-19: Formas de abordar la ciberseguridad en la aviación civil, exhortó a los Estados, entre otras cosas, a:

- Identificar las amenazas y los riesgos de posibles incidentes de ciberseguridad en las operaciones y los sistemas críticos de la aviación civil, y las graves consecuencias que pueden resultar de tales incidentes;
- Fomentar una interpretación común entre los Estados miembros de las ciberamenazas y riesgos y la formulación de criterios comunes para determinar cuáles bienes y sistemas son de carácter crítico y es preciso protegerlos;
- Fomentar la coordinación entre gobierno e industria con respecto a las estrategias, políticas y planes de ciberseguridad de la aviación, así como el intercambio de información para ayudar a identificar las vulnerabilidades críticas que sea necesario resolver;
- Formar y participar en asociaciones y mecanismos público-privados entre gobierno e industria, a nivel nacional e internacional, para compartir sistemáticamente la información sobre ciberamenazas, incidentes, tendencias y acciones de mitigación;
- Establecer políticas y destinar recursos cuando sea necesario para garantizar que los sistemas de aviación críticos tengan una arquitectura diseñada para ser segura; que sean

resilientes; que tengan métodos seguros de transferencia de datos que garanticen su integridad y confidencialidad; que tengan métodos de vigilancia, detección y notificación de incidentes y que se lleven a cabo análisis forenses de los incidentes.

1.7 Mientras avanzan las tareas en la OACI a través del Grupo de Trabajo INNOVA para establecer métodos comunes y mutuamente acordados para proteger a la comunidad aeronáutica de los riesgos de ciberseguridad a través de un marco unificado de requisitos regulatorios, algunos Estados han expresado su preocupación en relación al establecimiento e implantación de programas de ciberseguridad.

1.8 A fin de enfrentar estas inquietudes y dado el gran volumen de comunicación e información compartida entre la FAA y las autoridades de aviación civil y los proveedores de servicios de navegación aérea en el Caribe, la FAA está programando un simulacro de ciberseguridad para contribuir al desarrollo de mejores prácticas a nivel regional en respuesta a las ciberamenazas en la aviación. Este ejercicio podría servir de modelo para otros simulacros de ciberseguridad en el futuro.

1.9 El simulacro de ciberseguridad planificado será un debate facilitado de escenarios en un ambiente formal relajado. Será un intercambio abierto de ideas sobre distintos temas relacionados con un incidente de ciberseguridad hipotético simulado, y puede ser utilizado para mejorar la conciencia general, validar los actuales planes y procedimientos, y evaluar los sistemas y las actividades de respuesta y recuperación a los incidentes de ciberseguridad en la Región del Caribe. El ejercicio también se enfocará en la políticas, planes, contingencias de personal, compartición de información y coordinación gubernamental, e identificará cualquier brecha o responsabilidades poco claras o superpuestas.

1.10 El simulacro de ciberseguridad propuesto permitirá reunir a la FAA y a los Estados del Caribe para garantizar que los sistemas y redes de información independientes y compartidos funcionen en forma exitosa y sean resilientes a los incidentes de ciberseguridad.

1.11 Inicialmente, el simulacro de ciberseguridad está diseñado para generar una discusión de alto nivel, enfocada en la política y en los métodos. Los objetivos de este ejercicio son:

- Generar y fomentar una interpretación común de las ciberamenazas, vulnerabilidades y riesgos resultantes a través del ecosistema aeronáutico
- Identificar brechas en las políticas y operaciones del Estado
- Identificar y fomentar asociaciones y mecanismos regionales para compartir información sobre amenazas emergentes y respuesta a incidentes

3.0 Conclusión

3.1 Mientras continúan las labores en la OACI en relación a un marco unificado de requisitos regulatorios para fortalecer la ciberseguridad, se requiere un mayor esfuerzo a nivel estatal y regional. Trabajando juntos en las asociaciones regionales y utilizando un modelo exitoso para lograr una interpretación común e identificar brechas en las políticas y reglamentos, los Estados pueden empezar a desarrollar un marco básico para mejorar la ciberseguridad y mitigar los incidentes que la afectan.

4.0 Acción sugerida

4.1 Se invita a la reunión a:

a) tomar nota de la información contenida en esta nota; y

b) respaldar el concepto de simulacros de ciberseguridad a nivel regional, realizados en cooperación con las Oficinas Regionales de la OACI y los Estados miembros, tal como se indica en el párrafo 2.6, utilizando el debate facilitado de escenarios que permita un intercambio abierto de ideas sobre diversos temas relacionados con un incidente de ciberseguridad hipotético simulado. El ejercicio puede ser utilizado para mejorar la conciencia general, validar los planes y procedimientos existentes, y evaluar los sistemas y las actividades relacionados con la respuesta a los incidentes de ciberseguridad y la recuperación de los mismos.

- FIN -