Manual de participación

Ensayo de Ciber-Resiliencia de Navegación Aérea (TTX)

Descripción general del ejercicio

El ejercicio de ciber-resiliencia es una herramienta útil para probar la resiliencia existente de la navegación aérea y los procedimientos de comunicación.
V

Fecha de ejercicio: 09-12 de octubre de 2023
Ubicación: Lima, Perú
Anfitrión: Oficina Regional Sudamericana de la OACI (SAM)
Punto de contacto:

- *Roberto Sosa, OFICIAL REGIONAL, ATM Y SAR OSG/SAM. rsosa@icao.int*

Facilitadores:

- *Da Silva, Saulo, JEFE, SISTEMAS INTEROPERABLES GLOBALES, ANB/AN/GIS. sdasilva@icao.int*
- *Kornetskiy, Anton, OFICIAL TÉCNICO, SISTEMAS INTEROPERABLES GLOBALES, ANB/AN/GIS. AKornetskiy@icao.int*

Objetivos del ejercicio:

1. Reducir la confusión y agilizar la toma de decisiones durante las emergencias de ciberseguridad en la navegación aérea, permitiendo acciones rápidas y proactivas por parte del personal involucrado.
2. Desarrollar conciencia y promover una comprensión común de las vulnerabilidades de los sistemas de navegación aérea y los riesgos resultantes que afectan a las operaciones.
3. Empoderar a los participantes con medidas para mitigar la degradación de los sistemas mediante la identificación y promoción de mecanismos para el intercambio de información.
4. Introducir el *International Aviation Trust Framework* (IATF) y promover los beneficios globales para el ecosistema de la aviación al ser parte del (IATF).
5. Proporcionar orientación práctica sobre cómo desarrollar y ejecutar ejercicios adaptados al Estado/organización.

Temas de ejercicio:

- **Expectativas, habilidades y experiencia**
  - Rol, responsabilidades, autoridades e interacciones con los demás
- **Políticas y procedimientos**
  - Planes y procedimientos actuales e inconsistencias significativas, si las hay
- **Riesgos para la seguridad de las operaciones de vuelo**
  - Peligros y vulnerabilidades que podrían ser impactantes
- **Función del *International Aviation Trust Framework*.**

Programa de ejercicios

DÍA 1 (9 DE OCTUBRE DE 2023)		
Hora	**Actividad**	**Orador/Moderador**
0800 - 0900	Registro	
0900 - 0930	Sesión de apertura	OACI RO
0930 – 1015	Introducción	Sede de la OACI
1015 - 1045	*Foto de grupo y café / té*	
1045 - 1115	La perspectiva y las actividades regionales	OACI RO
1115 - 1215	Estableciendo el escenario de ciberseguridad	Sede de la OACI
1215 - 1315	*Almuerzo*	
1315 - 1415	International Aviation Trust Framework (IATF) Discusión (parte 1)	Sede de la OACI
1415 - 1430	*Pausa café/té*	
1430 - 1530	*International Aviation Trust Framework* (IATF) Discusión (parte 2) + Preguntas y respuestas	Sede de la OACI
DÍA 2 (10 DE OCTUBRE DE 2023)		
0900 – 0930	Resumen del trabajo del día anterior	Sede de la OACI
0930 - 1030	Introducción al ejercicio TTX	Todos
1030 - 1100	*Pausa café/té*	
1100 - 1200	Ejercicio TTX: Escenario 1	Todos
1200 - 1300	*Almuerzo*	
1300 - 1430	Ejercicio TTX: Escenario 1 (continuará)	Todos
1430 - 1445	*Pausa café/té*	
1445 - 1530	Ejercicio TTX: Escenario 2	Todos
DÍA 3 (11 DE OCTUBRE DE 2023)		
0900 – 0930	Resumen del trabajo del día anterior	Sede de la OACI
0930 - 1030	Ejercicio TTX: Escenario 2 (continuará)	Todos
1030 - 1100	*Pausa café/té*	
1100 - 1200	Ejercicio TTX: Escenario 3	Todos
1200 - 1300	*Almuerzo*	
1300 - 1400	Ejercicio TTX: Escenario 3 (continuará)	Todos
1400 - 1430	*Pausa café/té*	
1430 - 1530	Examen de TTX, lecciones aprendidas y mesa redonda de preguntas y respuestas	Sede de la OACI
	DÍA 4 (12 DE OCTUBRE DE 2023)	
0900 – 0915	Resumen del trabajo del día anterior	Sede de la OACI
0915 - 1045	Taller sobre Fundamentos de la Estrategia de Comunicación y Gestión de las Partes Interesadas	Sede de la OACI
1045 - 1115	*Pausa café/té*	
1115 - 1245	Cómo crear y ejecutar un ejercicio de mesa a la medida del estado / organización	Sede de la OACI
1245 - 1345	*Almuerzo*	
1345 - 1430	Resumen del taller y cierre	OACI

Términos y definiciones

Los términos y definiciones del presente documento son específicos de este ejercicio y pueden diferir de los presentados en otros documentos de la OACI. Son simplemente para aclarar los términos en el contexto de estos ejercicios.

Relacionados con la aviación:

- ***Dominio de la aviación V. Ecosistema de la aviación***

    - **Dominio de la aviación:** El espacio aéreo mundial, incluido el nacional e internacional, así como todas las aeronaves tripuladas y no tripuladas que operan en ese espacio aéreo, las personas y la carga presentes en ese espacio aéreo, y todas las infraestructuras relacionadas con la aviación.
    - **Ecosistema de Aviación:** Una red de múltiples capas de elementos que se cruzan con roles integrales en el Dominio de la Aviación e involucra seis entidades principales: Aeropuertos, Aerolíneas, Transporte Aéreo, Aeronaves, Actores y Gestión de Aviación.
- **Otros términos y definiciones de aviación**
    - **ANSP**: Utilizado genéricamente para todos los proveedores de servicios de navegación aérea.
    - **Aerolínea**: Se utiliza genéricamente para todas las compañías aéreas con pabellón (pasajeros, carga).
    - **AIRAC:** Proceso de sincronización de Regulación y Control de Información Aeronáutica.
- **Redes de Comunicaciones**: Responsable de los circuitos, redes y equipos de soporte de voz y datos (correo electrónico, vigilancia, planes de vuelo, etc.)
- **Licencia de piloto de drones:** Un certificado que los pilotos de drones deben llevar en todo momento mientras operan su dron.
- **Partes interesadas ejecutivas**: Líder sénior responsable de tomar decisiones políticas, "no rutinarias".
- ***International Aviation Trust Framework* (IATF):** Un conjunto de políticas, requisitos y mejores prácticas que permitirán el intercambio confiable, resistente y seguro tierra-tierra, aire-tierra y aire-aire de información digital entre todas las partes interesadas actuales y futuras de la aviación.
- **Partes interesadas en las operaciones**: Proporcionar servicios de tráfico aéreo y flujo de tráfico aéreo, responsable de tomar decisiones "rutinarias" basadas en políticas y procedimientos existentes.
- **ID remota de drones:** La capacidad de un dron en vuelo para proporcionar información de identificación y ubicación que puede ser recibida por otras partes a través de una señal de transmisión o un sistema basado en red.
- **Piloto remoto:** Una persona encargada por el operador de tareas esenciales para la operación de una aeronave pilotada a distancia y que manipula los controles de vuelo, según corresponda, durante el tiempo de vuelo.
- **Estado de registro:** Estado en cuyo registro se inscribe la aeronave.
    - Todas las aeronaves no tripuladas (UA) deben registrarse de acuerdo con la parte 101 del Reglamento Modelo de UAS de la OACI.
- **Sistema de aeronaves no tripuladas (UAS):** Una aeronave y sus elementos asociados que se operan sin piloto a bordo.
    - * La discusión contará con un pequeño dron (251 g -25 kg) equipado con una cámara digital profesional de una sola lente réflex (DSLR)

Relacionado con el ciberseguridad

- **Ciberhigiene:** Prácticas y pasos para mantener el estado del sistema informático y del dispositivo y mejorar la seguridad en línea.
- **Amenaza cibernética:** Una acción o evento negativo potencial facilitado por una vulnerabilidad que podría resultar en un impacto no deseado en un sistema o aplicación informática.
- **Denegación de servicio distribuida:** Una técnica de denegación de servicio que utiliza numerosos sistemas simultáneamente para perjudicar el uso autorizado de los recursos o servicios del sistema de información, generalmente inundando la red con paquetes de grandes cantidades de datos.
- **Evento:** Una ocurrencia observable en un sistema o red (por ejemplo, un usuario que envía correo electrónico).
- **Incidente:** Un evento adverso en un sistema o red de información, o la amenaza de tal evento.
- **Plan de respuesta a incidentes:** Una serie de acciones planificadas previamente que incluyen los procesos, procedimientos y documentación relacionados con la forma en que su organización detecta, responde y se recupera de los incidentes.
- **Malware:** Software que compromete el funcionamiento de un sistema mediante la realización de una función o proceso no autorizado.
- **Phishing**: Una forma digital de ingeniería social para engañar a las personas para que proporcionen información confidencial.
- **Resiliencia:** Capacidad para mantener la capacidad del sistema para entregar el resultado deseado continuamente en todo momento, incluso cuando los mecanismos de entrega regulares han fallado.
  Suplantación de identidad: falsificar la dirección de envío de una transmisión para obtener una entrada ilegal [no autorizada] en un sistema; la inducción deliberada de un usuario o recurso para que tome medidas incorrectas. Nota: Suplantar, enmascarar, llevar a cuestas e imitar son formas de suplantación de identidad.
- **Confianza cero:** La confianza cero es un marco de seguridad que requiere que todos los usuarios, ya sea dentro o fuera de la red de la organización, estén autenticados, autorizados y validados continuamente para la configuración y postura de seguridad antes de que se les otorgue o mantengan el acceso a aplicaciones y datos.

Funciones y responsabilidades del participante

El término participante abarca muchos grupos de personas, no solo aquellos que juegan en el ejercicio. Como mínimo, se requiere un moderador y jugadores. Los grupos de participantes que intervienen en el ejercicio, y sus respectivas funciones y responsabilidades, son los siguientes:

- **Moderador**: Dirige el flujo general durante la realización del ejercicio.
- **Expertos en la materia (SME):** Según se solicite, ayudar proporcionando información, análisis y recomendaciones relevantes en su área de especialización o proporcionando experiencia en la materia.
- **Jugadores:** Activos en la discusión o el desempeño de sus roles y responsabilidades regulares durante el ejercicio.
- **Grabadores**: Monitorean el flujo general de ejercicio y ayudan a documentar acciones y decisiones, en apoyo de la información / documentos posteriores al ejercicio.

- **Observadores:** Observar el flujo general del ejercicio de una manera que no afecte directamente su realización.

Estructura del ejercicio

1. **El escenario de discusión facilitado por IATF** se basará en la seguridad de las operaciones de UAS a nivel internacional y nacional. La intención de esta discusión es resaltar los beneficios globales para el ecosistema de la aviación al ser parte del International Aviation Trust Framework**.**

    - Se anima a los partipantes a interactuar activamente de acuerdo con sus acciones, responsabilidades, políticas y experiencia del mundo real.

2. **El escenario Cyber Resilience TTX** se basará en el **proceso de Gestión del Plan de Vuelo** y se presentará en tres partes (3 escenarios más varias adiciones). La intención de estas adiciones es resaltar la interconexión de los sistemas cibernéticos con la infraestructura física y ejercer la coordinación y la comunicación entre las partes interesadas. Después de cada parte, los participantes tendrán un tiempo establecido para revisar el módulo y debatir las preguntas de discusión. **El escenario TTX de resiliencia cibernética** tiene tres objetivos principales :

        - Para interrumpir sistemas específicamente dirigidos a través de eventos de ciberseguridad (críticos o de otro tipo)
        - Comprometer los sistemas para obtener ganancias financieras
        - Socavar la confianza pública en los viajes aéreos

    - Los moderadores presentarán la situación y los participantes discutirán sobre las acciones de respuesta apropiadas y los problemas que surgen del escenario en cuestión.
    - Los participantes pueden formar equipos para facilitar las discusiones.
    - La situación tendrá una serie de parámetros que se agregaran a lo largo de la narrativa. El objetivo es cambiar una o más variables en la situación presentada o avanzar en la historia.
    - El escenario concluirá cuando la historia esté terminada o cuando se hayan cumplido los objetivos de la situación.
    - A continuación, se introducirá la siguiente situación (según corresponda). Las situaciones posteriores pueden basarse en situaciones anteriores o pueden no estar relacionadas en absoluto.

3. **Taller de Fundamentos de Estrategia de Comunicación y Gestión de Grupos de Interés.**

    - Los moderadores utilizarán escenarios discutidos previamente durante el TTX, junto con varias herramientas de gestión de proyectos, para proporcionar a los participantes orientación práctica en el desarrollo de una estrategia de comunicación personalizada como parte de su plan de respuesta a incidentes.
    - Los asistentes participarán en actividades grupales.
    - Se anima a los participantes a responder al escenario utilizando su conocimiento de los planes de comunicación actuales, las estrategias y el conocimiento recibido durante el TTX.

4. El **"Taller de ejercicios adaptados a los Estados/Organizaciones"** ayudará a los Estados Miembros de la OACI y a otras partes interesadas del ecosistema de la aviación a crear y realizar ejercicios para evaluar su capacidad de planificar, responder y recuperarse de incidentes cibernéticos.

- Este taller equipa a los participantes con medidas para prevenir la degradación de sistemas críticos de navegación aérea, mejora la conciencia de los problemas cibernéticos en la aviación y promueve el uso seguro y resiliente del sistema.
- Los moderadores presentarán un conjunto de mejores prácticas y ejemplos para proporcionar a los participantes una hoja de ruta sólida para iniciar, planificar, diseñar, realizar, evaluar y mejorar los TTX.

Observaciones importantes

Los participantes no tienen conocimientos avanzados de los escenarios y recibirán toda la información al mismo tiempo.
Aunque se basa en un escenario plausible, este TTX no pretende replicar un ataque real o simular una respuesta completa. El objetivo es examinar y debatir la coordinación de incidentes y los problemas de comunicación en lugar de determinar una "mejor" respuesta.

Aunque se utilizan términos generales en el escenario, los participantes deben sumergir en el ejercicio como si estuviera sucediendo en su región y en su espacio aéreo. Los participantes siempre deben tener en cuenta que el escenario presentado es ficticio y los nombres mencionados solo se usan para el contexto o como ejemplos. Los participantes deben tener en cuenta que los escenarios presentados se basan en ciertas suposiciones que pueden ser diferentes de su propio estado o región. Si este es el caso, siéntase libre de señalar las diferencias y discutirlas.

Este ejercicio se llevará a cabo en un ambiente abierto, de bajo estrés. Se esperan y alientan diversos puntos de vista, incluso desacuerdos.

Durante todas las actividades:

- Responda al escenario utilizando su propio conocimiento de los planes, políticas y capacidades actuales (es decir, puede usar solo activos existentes) e información. No se requieren otros recursos para participar activamente en el TTX.
- Utilice activamente la **herramienta Slido.com** cuando los moderadores se lo pidan que proporcione sus respuestas / ideas.
- “Piensa fuera de la caja”. No hay una respuesta correcta o incorrecta. Se recomienda encarecidamente a los participantes que se involucren en las discusiones, ya que el propósito principal del ejercicio es intercambiar conocimientos y compartir experiencias.
- Discutir y presentar múltiples opciones y posibles soluciones. Las decisiones no sientan precedentes y pueden no reflejar su posición final sobre un tema determinado.
- Identifique problemas, pero también sugiera y recomiende acciones que podrían mejorar los esfuerzos de ciberseguridad . Los esfuerzos de resolución de problemas deben ser el foco del ejercicio.

No debe haber difusión de materiales de ejercicio o discusión; *La comunicación debe permanecer en la habitación*. Los resultados de la discusión se distribuirán a todos los participantes y observadores y podrán compartirse libremente. Ningún Estado, organización o persona será atribuido directamente a los resultados de la discusión.