OACI

Doc 10213 – Para distribución pública

Consideraciones sobre ciberriesgos mundiales

Primera edición, 2025

Aprobado por el Secretario General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

OACI

Doc 10213 – Para distribución pública

Consideraciones sobre ciberriesgos mundiales

Primera edición, 2025

Aprobado por el Secretario General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

Publicado por separado en español, árabe, chino, francés, inglés y ruso
por la ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL
999 Robert-Bourassa Boulevard, Montréal, Québec, Canada H3C 5H7

La información sobre pedidos y la lista completa de las agencias de ventas
y librerías pueden obtenerse en el sitio web de la OACI: www.icao.int

Primera edición, 2025

Doc 10213, *Consideraciones sobre ciberriesgos mundiales*

Número de pedido: 10213-U
ISBN 978-92-9275-970-4

ENMIENDAS

La publicación de enmiendas se anuncia periódicamente en los suplementos del *Catálogo de productos y servicios;* el Catálogo y sus suplementos pueden consultarse en el sitio web de la OACI: www.icao.int. Las casillas en blanco facilitan la anotación de estas enmiendas.

REGISTRO DE ENMIENDAS Y CORRIGENDAS

ENMIENDAS		
Núm.	Fecha	Anotada por

CORRIGENDAS			
Núm.	Fecha	Idioma	Anotada por

Las *Consideraciones sobre ciberriesgos mundiales* (Doc 10213 – Distribución limitada) de la OACI contienen información de distribución limitada; su uso está restringido a los gobiernos, la industria y otras partes interesadas de la aviación que se ocupan de la ciberseguridad con el fin de evaluar riesgos. Esta versión del Doc 10213 es un extracto apto para su distribución al público.

PREÁMBULO

En las últimas décadas, se ha observado una rápida evolución en el uso de la información y las nuevas tecnologías en el sector de la aviación civil para contribuir a las metas de automatización, interconectividad e interoperabilidad. Esta tendencia se ha acelerado más recientemente, en particular, en las áreas operacionales que aprovechan los últimos avances tecnológicos, como el aprendizaje automático y el análisis de macrodatos. La digitalización acelerará la implementación de nuevos conceptos operacionales en tierra y en el aire e integrará nuevos elementos, como los sistemas de aeronaves no tripuladas (UAS), en el sistema del transporte aéreo. El objetivo fundamental de estos avances es estimular el crecimiento del sector de la aviación civil y, a su vez, mejorar su seguridad, protección, eficiencia, capacidad y sostenibilidad.

Sin embargo, con esta tendencia, el panorama de ciberamenazas llegó a los sistemas e información operacionales, lo que puede tener efectos adversos en la seguridad, la protección, la capacidad y/o la eficiencia de la aviación civil. Así, el sector de la aviación se ha visto obligado a hacer frente a las ciberamenazas y ciberriesgos para la aviación civil más allá del contexto tradicional de la seguridad de la tecnología de la información y la tecnología operacional (IT/OT) integrando la gestión de ciberriesgo en la aviación en los procesos de gestión de riesgos de la aviación de todas las disciplinas de la aviación civil, con el fin de procurar la protección y la resiliencia del sistema de transporte aéreo mediante marcos de gestión de riesgo sólidos y eficaces.

El presente documento, *Consideraciones sobre ciberriesgos mundiales,* fue elaborado por la Organización de Aviación Civil Internacional (OACI) para prestar asistencia a los Estados miembros y las partes interesadas en la integración de la gestión de ciberriesgos en los procesos de gestión de riesgos de la aviación. También ofrece un panorama mundial de alto nivel de las ciberamenazas para destacar la importancia de hacer frente a las ciberamenazas y ciberriesgos a la aviación civil, a fin de posibilitar un sector resiliente y protegido.

Este documento pretende promover el cumplimiento por los Estados y las partes interesadas de las obligaciones de evaluación de riesgos establecidas en los Anexos del Convenio sobre Aviación Civil Internacional (Convenio de Chicago), en particular, la norma 4.9.1 del Anexo 17 – *Seguridad de la aviación*. También promueve la implementación de la Estrategia de Ciberseguridad de la Aviación[1] de la OACI y su correspondiente Plan de Acción de Ciberseguridad[2].

La información contenida en este documento responde a los principios generales de las orientaciones de la OACI sobre los procesos de gestión y evaluación de riesgos de seguridad operacional y seguridad de la aviación, tal como se describe en la *Declaración del contexto mundial de riesgo para la seguridad de la aviación* (Doc 10108 – Distribución limitada), el *Manual de seguridad de la aviación* (Doc 8973 – Distribución limitada) y el *Manual de gestión de la seguridad operacional* (Doc 9859).

Asimismo, se incluyen varios apéndices que contienen ejemplos de aplicación de la metodología de gestión de ciberriesgos en la evaluación de riesgos de seguridad operacional y seguridad de la aviación. Los apéndices también contienen orientación sobre la categorización de las ciberamenazas, que ha sido diseñada para ayudar a los Estados y a las partes interesadas a detectar interdependencias y vínculos entre las diferentes disciplinas de la aviación. Con ello, se pretende facilitar la formulación y el mantenimiento de un marco de gestión de riesgos sólido en aviación civil.

Agradecemos a las personas miembros del Grupo Experto en Ciberseguridad y su Grupo de Trabajo sobre Ciberamenazas y Ciberriesgos por haber aportado su tiempo y conocimientos valiosos para elaborar este documento.

1. Véase https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx
2. Véase https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx

ÍNDICE

ABREVIATURAS Y ACRÓNIMOS

ANSP	Proveedor de servicios de navegación aérea
APT	Amenaza persistente avanzada
ATC	Control de tránsito aéreo
AVSEC	Seguridad de la aviación
CPDLC	Comunicaciones por enlace de datos controlador/a-piloto/a
CRC	Verificación por redundancia cíclica
DDoS	Denegación de servicio distribuida (DDoS)
DPI	Derecho de propiedad intelectual
EATM-CERT	Equipo europeo de respuesta a emergencias informáticas de gestión del tránsito aéreo
EFB	Maletín de vuelo electrónico
FTA	Análisis de árbol de fallas
GNSS	Sistema mundial de navegación por satélite
HVAC	Calefacción, ventilación y aire acondicionado
IP	Protocolo de Internet
IT/OT	Tecnología de la información/Tecnología operacional
MET	Meteorología/Servicios meteorológicos
NEASCOG	Grupo OTAN-EUROCONTROL de coordinación de la seguridad en la gestión del tránsito aéreo (ATM)
PBIED	Artefacto explosivo improvisado que una persona lleva oculto
PII	Información de identificación personal
UAS	Sistema(s) de aeronaves no tripuladas

Capítulo 1

DEFINICIONES

Agente de amenaza (o actor). Entidad que es parcial o totalmente responsable de un incidente que afecta, o tiene el potencial de afectar, a una organización o sistema.

Ciberactivo. Elementos digitales y físicos que tienen valor en términos de negocio, operaciones, seguridad operacional, protección, eficiencia y/o capacidad de la aviación, como sistemas, información, datos, redes, dispositivos, *software*, *hardware*, procesos, *firmware*, personal relevante/personal certificado y otros recursos electrónicos.

Ciberamenaza. Cualquier posible cibersuceso susceptible de afectar negativamente a la seguridad operacional, la protección, la eficiencia y/o la capacidad de la aviación.

Ciberataque. El uso deliberado de medios electrónicos para interrumpir, alterar, destruir u obtener acceso no autorizado a ciberactivos.

Ciberincidente. Suceso, serie de sucesos de ciberseguridad, que afecten negativamente a la seguridad operacional, la protección, la eficiencia y/o la capacidad de la aviación.

Cibermitigación. Control o controles de seguridad que tienen por objeto reducir el riesgo de ciberseguridad asociado a una ciberamenaza o vulnerabilidad específica, teniendo en cuenta su impacto en la seguridad operacional, la protección, la eficiencia y/o la capacidad de la aviación.

Ciberresiliencia. Capacidad de un ciberactivo de mantener funciones críticas en condiciones adversas o estrés, y para recuperarse de esas condiciones adversas.

Ciberriesgo. Posibilidad de un resultado no deseado como resultado de un cibersuceso.

Ciberseguridad de la aviación. Conjunto de tecnologías, controles y medidas, procesos, procedimientos y prácticas diseñados para garantizar la confidencialidad, integridad, disponibilidad y protección general y resiliencia de los ciberactivos frente a ataques, daños, destrucción, interrupciones, accesos no autorizados y/o explotación.

Cibersuceso. Cualquier ocurrencia observable en una red o sistema.

Confidencialidad. Propiedad que impide que un activo se ponga a disposición de, o se divulgue a, una persona, un usuario, un programa, un proceso, un sistema o un dispositivo no autorizado.

Control del acceso. Medidas diseñadas para que solo se otorgue acceso autorizado a los activos físicos y a los ciberactivos.

Disponibilidad. Condición de ser accesible y utilizable, a pedido, por una persona, un usuario, un programa, un proceso, un sistema o un dispositivo titular de una autorización.

Evaluación del ciberriesgo. Proceso continuo de identificación, análisis y evaluación de ciberriesgos.

Fiabilidad. Propiedad que permite que un activo realice, en el nivel esperado, una función requerida en condiciones especificadas, sin fallos, durante un período de tiempo especificado.

Gestión del ciberriesgo. Proceso continuo de identificación, mitigación, tratamiento y monitoreo de ciberamenazas y ciberriesgos, de acuerdo con una evaluación de riesgos.

Gravedad. Indicación cualitativa de la magnitud del efecto adverso de una condición de amenaza.

Infraestructura crítica de aviación. Activos que son tan esenciales que su inhabilitación, compromiso o destrucción tendría un impacto debilitante en la seguridad operacional, la seguridad de la aviación, la eficiencia y/o la capacidad de la aviación.

Integridad. Propiedad de exactitud y cabalidad de un activo, que fundamenta lo que se supone que es dicho activo.

Matriz de ciberriesgos. Herramienta para clasificar y mostrar los componentes de los riesgos (probabilidad, amenaza, impacto/consecuencia y vulnerabilidad), las mitigaciones de riesgos y, en última instancia, los riesgos residuales.

Perturbación. Cibersuceso, ya sea anticipado o imprevisto, que causa una desviación negativa no planificada de las operaciones normales.

Vector de ataque. Medio de acceso que utilizó un/una atacante para iniciar un ataque.

Capítulo 2

METODOLOGÍA PARA INTEGRAR LA GESTIÓN DEL CIBERRIESGO EN LOS MARCOS DE GESTIÓN DE RIESGOS DE AVIACIÓN

Nota 1.— En este capítulo, por funciones de aviación *se entienden las funciones de las distintas disciplinas de la aviación que tienen integrada la gestión de ciberriesgos en sus procesos de gestión de riesgos, es decir, la seguridad operacional, la seguridad de la aviación, la eficiencia de la navegación aérea y/o la capacidad de la navegación aérea. En el mismo contexto, las funciones críticas de la aviación son funciones que se consideran fundamentales para las disciplinas de aviación en cuestión.*

Nota 2.— En este capítulo, el término especialistas en gestión de riesgos de aviación *se refiere a especialistas en gestión de riesgos relacionados con la seguridad operacional, la seguridad de la aviación y la eficiencia y/o capacidad de la navegación aérea, y los procesos de gestión de riesgos de aviación son los procesos de gestión de riesgos de estas disciplinas de aviación.*

2.1 OBJETIVOS

2.1.1 El objetivo de este capítulo es ayudar a los Estados y las partes interesadas en sus procesos de gestión de riesgos, desde la identificación hasta el tratamiento y examen de riesgos; a tal efecto, se recomienda una metodología genérica para integrar la evaluación y gestión de los ciberriesgos en los marcos existentes de gestión de riesgos de seguridad operacional, seguridad de la aviación y eficiencia y capacidad de la navegación aérea.

Nota 1.— Aunque la metodología abarca la integración de la gestión de ciberriesgos en las evaluaciones de seguridad operacional, seguridad de la aviación y eficiencia y capacidad de la navegación aérea, se puede adaptar para aplicarla a cualquier otra disciplina de la aviación civil (como la gestión de riesgos de las actividades).

. *Nota 2.— Antes de aplicar la metodología presentada en este capítulo, los Estados y las partes interesadas podrían considerar aquellas áreas que ya cuentan con metodologías de evaluación de riesgos y que las autoridades competentes reconocen comúnmente como medios aceptables de cumplimiento de sus requisitos reglamentarios específicos de la aviación, como las evaluaciones de riesgos relacionadas con la certificación de aeronaves.*

2.1.2 Este capítulo está dirigido al grupo de especialistas en gestión de riesgos de seguridad operacional, seguridad de la aviación, navegación aérea y ciberriesgos que deberían trabajar en colaboración para integrar la gestión de los ciberriesgos en sus respectivos marcos de gestión de riesgos de aviación en todas las disciplinas de la aviación civil.

2.2 DESCRIPCIÓN GENERAL

2.2.1 La metodología presentada en este documento sigue los conceptos generales del ciclo de gestión de riesgos que se representan en la figura 1.

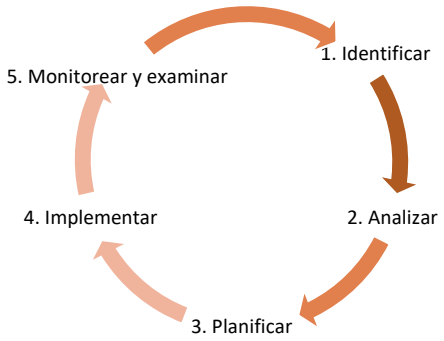


Figura 1. Ciclo de gestión de riesgos

2.2.2 La metodología se desarrolla a partir de textos de orientación de la OACI relativos a la evaluación de riesgos, a saber, el *Manual de gestión de la seguridad operacional* (Doc 9859) y la *Declaración del contexto mundial de riesgo para la seguridad de la aviación* (Doc 10108 – Distribución limitada). La metodología tiene en cuenta el trabajo de diferentes grupos expertos de la OACI, así como las aportaciones del Grupo OTAN-EUROCONTROL de coordinación de la seguridad en la gestión del tránsito aéreo (ATM), y también está alineada con las normas internacionales sobre gestión de ciberriesgos (ISO/IEC 27001:2022 [3], ISO 31000:2018 [4], EUROCAE/RTCA ED201A/DO-391[5] y NIST SP 800-30 Rev.1[6]).

2.2.3 Con la aplicación de la metodología a las evaluaciones existentes de riesgos de aviación de las funciones críticas de aviación, se obtendrán los siguientes resultados:

- una evaluación actualizada de los riesgos de seguridad operacional que incluye la evaluación de los ciberriesgos pertinentes;
- una evaluación actualizada de los riesgos de seguridad de la aviación que incluye la evaluación de los ciberriesgos pertinentes;
- una evaluación actualizada de los riesgos de eficiencia de la navegación aérea que incluye la evaluación de los ciberriesgos pertinentes; y/o
- una evaluación actualizada de los riesgos de capacidad de la navegación aérea que incluye la evaluación de los ciberriesgos pertinentes.

2.2.4 Antes de aplicar la metodología, es esencial que especialistas en aviación determinen cuáles son las funciones críticas de aviación en la disciplina que se está evaluando. Para ello, pueden efectuarse consultas, encuestas, etc., teniendo en cuenta los requisitos reglamentarios y jurídicos aplicables a la aviación, así como la infraestructura crítica nacional.

3. Véase https://www.iso.org/standard/27001.
4. Véase https://www.iso.org/standard/65694.html
5. Véase https://www.eurocae.net/product/ed-201a-aeronautical-information-system-security-aiss-framework-guidance/ o https://www.rtca.org/security/.
6. Véase https://csrc.nist.gov/pubs/sp/800/30/r1/final.

Nota.— La determinación de las funciones críticas de aviación y sus datos, información y sistemas de apoyo, en combinación con la aplicación de la metodología, contribuirá a las medidas que apliquen los Estados para cumplir sus obligaciones en virtud de la norma 4.9.1 del Anexo 17 – Seguridad de la aviación[7].

2.2.5 La metodología que se ilustra en la figura 2 debería incluir los siguientes pasos:

- **Paso 1** – Este paso debe ser realizado por especialistas pertinentes en riesgos de aviación en colaboración con ciberespecialistas.
  - ⇨ Comenzar con una evaluación ya existente de los riesgos de aviación de una función crítica de aviación.
  - ⇨ La evaluación de los riesgos de aviación proporcionará:
    - un nivel mínimo aceptable de seguridad operacional, llamado nivel deseado de seguridad operacional;
    - un riesgo residual de seguridad de la aviación;
    - un nivel mínimo deseado de capacidad; y/o
    - un nivel mínimo deseado de eficiencia.
  - ⇨ Determinar los datos, la información y los sistemas que respaldan la función crítica de aviación y cuya manipulación podría afectar la seguridad operacional, la seguridad de la aviación, la eficiencia y/o la capacidad de la aviación civil.

Nota.— En caso de que se identifique una función crítica de aviación para la que no exista una evaluación de riesgos, debería realizarse la evaluación de riesgo de aviación pertinente y utilizarla en el paso 1. Mientras tanto, se puede realizar el paso 2 que figura a continuación para evaluar el riesgo relativo a los datos, la información y los sistemas que respaldan esa función.

- **Paso 2** – *Este paso debe estar a cargo de ciberespecialistas en colaboración con especialistas en riesgos de aviación pertinentes*.
  - ⇨ Definir las hipótesis de ciberamenazas que podrían afectar los datos, la información y los sistemas del paso previo y realizar una evaluación de ciberriesgos de esas hipótesis.
    - Describir la hipótesis de amenaza, incluidos los medios y métodos de ciberataque y el tipo de actor.
    - Debería evaluarse la probabilidad primero sin tener en cuenta las medidas de mitigación actuales. Esto permite evaluar la intención y la capacidad del actor malintencionado para ejecutar la hipótesis de amenaza. Este paso podría incluir una descripción, en la medida de lo posible, del perfil del actor, de sus herramientas, etc.

Nota: Las ciberamenazas identificadas deberían ser objeto de monitoreo continuo para tener en cuenta los cambios de intención y/o de capacidad de los actores de amenazas.

- El impacto, la consecuencia o el efecto[8] se evalúa en función de la naturaleza y dimensión del ataque específico, en relación con la seguridad operacional, la seguridad de la aviación, la capacidad de la navegación aérea y/o la eficiencia de la navegación aérea, y teniendo en cuenta el peor de los casos razonablemente posibles o el peor de los casos verosímiles.
- La evaluación de las vulnerabilidades restantes del sistema considera la aplicación de las medidas de mitigación existentes.
- El resultado de esta evaluación es el ciberriesgo residual. Es el riesgo global que queda después de haber considerado las mitigaciones existentes y de haber tenido en cuenta la probabilidad y las consecuencias de la amenaza.

7. Los Anexos del Convenio de Chicago, incluido el Anexo 17 y su norma 4.9.1, son aplicables a los Estados y no a determinadas disciplinas de la aviación, a menos que así se especifique. La norma 4.9.1 invoca a "los explotadores o entidades definidos en el programa nacional de seguridad de la aviación civil u otra documentación nacional pertinente". Esta redacción hace que la disposición sea aplicable a todas las disciplinas de la aviación definidas a nivel nacional por cada Estado.

8. Los términos *impacto*, *efecto* y *consecuencia* se utilizan indistintamente en este documento.

Nota 1.— Las tablas de probabilidad, impacto y clasificación de la vulnerabilidad restante se describen en la sección siguiente.

Nota 2.— Cada organización debería definir sus propios objetivos de ciberseguridad y criterios de aceptación de ciberriesgos a partir de los marcos reglamentarios y jurídicos aplicables, relativos o no a la aviación (por ejemplo, la autoridad nacional de ciberseguridad), así como de sus propios niveles de tolerancia al riesgo.

- **Paso 3** – *Este paso debe ser efectuado por especialistas en riesgos de aviación*.
  - ⇨ Actualizar la evaluación de riesgos de aviación indicada en el paso 1. Este paso dará como resultado:
    - un nivel de seguridad operacional actualizado;
    - un riesgo residual de seguridad de la aviación actualizado;
    - un nivel de capacidad actualizado; y/o
    - un nivel de eficiencia actualizado.

- **Paso 4** – *Este paso debe ser realizado conjuntamente por especialistas en riesgos de aviación y ciberespecialistas.*
  - ⇨ Evaluar los resultados actualizados de la evaluación de riesgos de aviación respecto de los niveles de riesgo originales obtenidos en el paso 1.
  - ⇨ Los criterios de aceptación de riesgos deberían estar predeterminados por la organización, ser exhaustivos y cubrir como mínimo las disciplinas de aviación pertinentes (seguridad operacional, seguridad de la aviación, capacidad y/o eficiencia) y los objetivos y metas de ciberseguridad.

Nota.— Cada organización debería definir sus propios objetivos de ciberseguridad y criterios de aceptación de ciberriesgos a partir de los marcos reglamentarios y jurídicos aplicables, relativos o no a la aviación (por ejemplo, la autoridad nacional de ciberseguridad), así como de sus propios niveles de tolerancia al riesgo.

  - ⇨ Tras la evaluación de los resultados actualizados respecto de los resultados originales obtenidos en el paso 1, el riesgo actualizado de la evaluación de riesgos de aviación debería considerarse inaceptable si:
    - la evaluación actualizada del riesgo de aviación no cumple las metas aceptadas (niveles de riesgo originales) obtenidas en el paso 1; o
    - el ciberriesgo residual no cumple los objetivos de ciberseguridad de la organización.
  - ⇨ Si el riesgo actualizado no es aceptable, la organización debería mitigar el riesgo agregando cibermitigaciones específicas cuando sea posible y reevaluar la aceptación del riesgo.
  - ⇨ Si, incluso después de aplicar cibermitigaciones, el riesgo sigue siendo inaceptable, la organización debería definir mitigaciones nuevas, pertinentes y eficaces para llevar el riesgo a niveles aceptables.

Nota.— En caso de discrepancia entre especialistas en la aviación y ciberespecialistas con respecto a la aceptabilidad del riesgo, la decisión debería elevarse al nivel ejecutivo de la organización.

  - ⇨ Si se han previsto cibermitigaciones, regresar al paso 3.
  - ⇨ Asegurarse de que las nuevas medidas de cibermitigación no tengan un impacto negativo sobre la evaluación de los riesgos de aviación. De ser necesario, tomar medidas de aviación[9] o reconsiderar las medidas de ciberseguridad para enfrentar cualquier impacto negativo.

9. Las *medidas de aviación* se refieren a medidas operacionales de seguridad operacional, seguridad de la aviación y eficiencia y/o capacidad de la navegación aérea.

Nota.— Es importante considerar el posible efecto de las cibermitigaciones sobre datos, información y/o sistemas críticos de otras funciones críticas de la aviación, ya que estas medidas pueden incidir en esas funciones. Si se observan efectos de ese tipo, debería llevarse a cabo una evaluación conjunta de los riesgos de aviación y los ciberriesgos asociados a esas funciones críticas.

⇨ La evaluación debería repetirse por las razones siguientes:

- la evolución de las ciberamenazas, como hipótesis de ciberamenazas existentes o nuevas que pueden volverse plausibles con el tiempo, cambios en la información o el conocimiento utilizado para determinar, analizar y clasificar riesgos;
- cambios en los requisitos relacionados con la evaluación de riesgos en las disciplinas en las que están integrándose los ciberriesgos;
- cambios funcionales en las funciones de aviación evaluadas; y/o
- cambios en el apetito de riesgo de la organización y la política de monitoreo y evaluación continuos y/o la recurrencia de la evaluación de riesgos.

2.2.6 Los apéndices A y B contienen dos ejemplos de cómo aplicar la metodología. En el primer ejemplo, en el **apéndice A,** se muestra cómo integrar una ciberamenaza en una evaluación de riesgos de seguridad operacional. El segundo ejemplo, **apéndice B,** muestra cómo integrar una ciberamenaza en una evaluación de riesgos de seguridad de la aviación.

2.2.7 El objetivo de estos ejemplos es demostrar que las evaluaciones de los riesgos de aviación y las evaluaciones de los ciberriesgos no pueden realizarse de forma aislada cuando se consideran las ciberamenazas a los procesos de aviación. **Es esencial que en las evaluaciones haya interacción, coordinación y colaboración para brindar una protección y resiliencia integrales a la aviación civil frente a las ciberamenazas y los ciberriesgos.**

2.3 MAPA DEL PROCESO METODOLÓGICO Y TABLAS DE PUNTUACIÓN DE CIBERRIESGOS

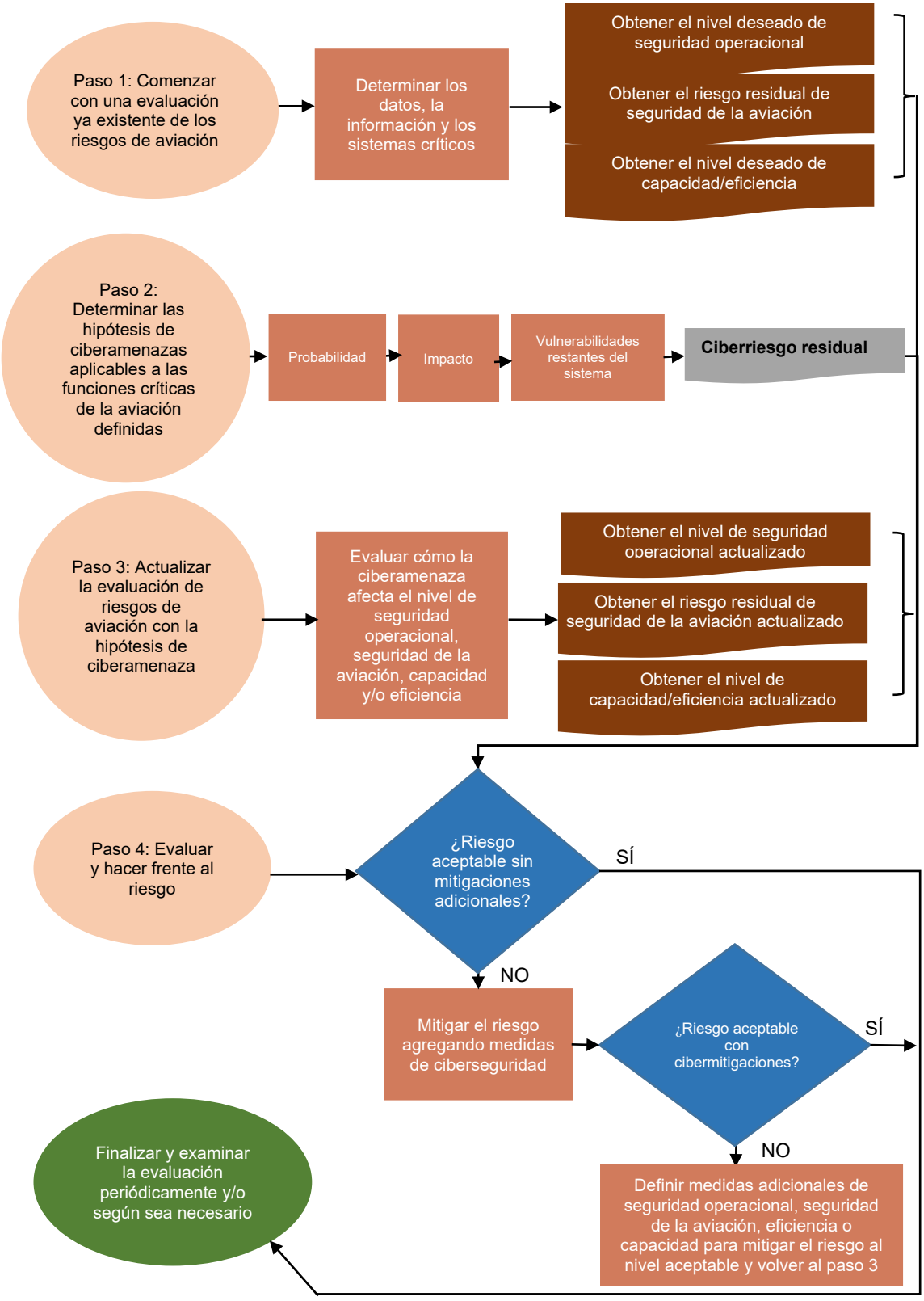


Figura 2. Mapa del proceso metodológico de gestión de riesgos

Tablas de puntuación de ciberriesgos

2.3.1 Las diversas tablas de puntuación de esta sección se proporcionan como mejores prácticas y orientaciones para crear matrices de evaluación de ciberriesgos. Aunque se recomienda su uso para la comprensión mutua de las ciberamenazas y ciberriesgos en el contexto de la compartición de la información[10], estas tablas de puntuación se pueden adaptar según las estrategias de gestión de riesgos de las organizaciones.

2.3.2 Las puntuaciones de esta sección se utilizan para elaborar las evaluaciones del capítulo 3 de la versión de distribución limitada de este documento.

2.3.3 En esta metodología, la probabilidad, el impacto y la vulnerabilidad se clasifican en cinco niveles (BAJO, MEDIO-BAJO, MEDIO, MEDIO-ALTO, ALTO). A cada nivel le corresponde una puntuación y una definición.

Probabilidad

2.3.4 La *probabilidad* se refiere a la posibilidad de que se produzca una ciberamenaza, teniendo en cuenta la capacidad y la intención de un actor de amenaza para llevar a cabo el ciberataque.

2.3.5 La evaluación de la probabilidad debería estar a cargo de ciberespecialistas, o al menos personas expertas en riesgos de la aviación que tengan acceso a informes de inteligencia sobre ciberamenazas.

Tabla 1. Clasificación de la probabilidad de ciberamenazas

CALIFICACIÓN DE PROBABILIDAD		
ALTA	5	Hipótesis muy plausible, en que un ataque real de este tipo ya haya ocurrido en los últimos años, o indicios sólidos de capacidad e intención para realizarlo.
MEDIA-ALTA	4	Hipótesis claramente plausible, para la que se posean ejemplos o pruebas relativamente recientes de primeras etapas de planificación de ataques o reconocimiento hostil.
MEDIA	3	Hipótesis esencialmente plausible, con algunos indicios de intención y capacidad para realizar un ataque y posiblemente algunos ejemplos de este.
MEDIA-BAJA	2	Hipótesis respecto de la cual no hay antecedentes o los hay pero no son recientes, pero en la que sí existe evidencia de intención, aunque con un método que aparentemente no está suficientemente desarrollado para un escenario de ataque certero o que probablemente ha sido remplazado por otras formas de ataque.
BAJA	1	Hipótesis teóricamente plausible, pero para la cuál no se cuenta con ejemplos, y en la que existe una intención teórica, pero ninguna capacidad aparente.

10. Para más información sobre la compartición de ciberinformación, véanse los textos de orientación sobre compartición de ciberinformación en el siguiente enlace: https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx

Impacto/Consecuencia/Efecto

2.3.6 El *impacto* es el resultado de medir en términos cualitativos las consecuencias de un ciberincidente en los activos mencionados en la descripción de una hipótesis de amenaza.

2.3.7 La evaluación del impacto debe estar a cargo de personas expertas en aviación de la función de aviación que se esté analizando.

2.3.8 Los impactos de las ciberamenazas en la seguridad operacional y la protección de la aviación se toman de los textos de orientación de la OACI sobre evaluación de riesgos de seguridad operacional de la aviación y para la seguridad de la aviación, respectivamente, del Manual de Gestión de la Seguridad Operacional (Doc 9859) y de la Declaración del Contexto Mundial de Riesgo para la Seguridad de la Aviación (Doc 10108 - Distribución limitada). El texto sobre el impacto en la capacidad y la eficiencia de la navegación aérea se elaboró para este documento.

Tabla 2. Clasificación del impacto de una ciberamenaza

CALIFICACIÓN DE IMPACTO/CONSECUENCIA/EFECTO[11]			
	Seguridad operacional de la aviación[12]	**Protección de la aviación[13]**	**Capacidad y/o eficiencia de la navegación aérea**
ALTO **Puntuación = 5**	**Catastrófico:** - Aeronave destruida	- Cientos de personas fallecidas - Miles de millones de dólares estadounidenses - Perturbación grave del servicio y de la confianza en el sistema de aviación	- Interrupción crítica de la capacidad y/o eficiencia de la navegación aérea. - Interrupciones generalizadas o fallos completos de los sistemas operacionales clave, que afectan gravemente a la gestión del tránsito aéreo o a las operaciones de aeropuertos[14] o de líneas aéreas[15]. - Retrasos prolongados o cancelación de vuelos, que plantean riesgos operacionales significativos para el sistema de aviación y la capacidad de operar aeronaves.
MEDIO-ALTO **Puntuación = 4**	**Peligroso:** - Lesión grave - Daños importantes - Una gran reducción del margen de seguridad operacional de modo que no se puede confiar en que el personal de operaciones realice sus tareas con precisión o en su totalidad.	- Algunos, pero no todos, los impactos de las consecuencias de nivel ALTO	- Interrupciones significativas en la capacidad y/o eficiencia de la navegación aérea. - Interrupciones prolongadas o fallas en sistemas operacionales clave, que repercuten en los servicios esenciales y la capacidad para operar aeronaves. - Retrasos sustanciales en la afluencia del tránsito aéreo o en las operaciones aeroportuarias o de las líneas aéreas, lo que causa congestión.

11. La tabla de calificación de impacto/consecuencia/efecto describe el impacto para cada disciplina de la aviación en la que se utiliza la metodología. Las columnas son independientes entre sí sobre la base de cada disciplina de la aviación, y la puntuación de la primera columna debería leerse junto con la columna específica de la disciplina de la aviación donde se integra la evaluación de ciberriesgos.
12. El impacto/consecuencia/efecto en la seguridad operacional de la aviación se tomó de la cuarta edición del *Manual de Gestión de la Seguridad Operacional* (Doc 9859).
13. El impacto/consecuencia/efecto en la seguridad de la aviación se tomó de la tercera edición de la Declaración del *Contexto Mundial de Riesgo para la Seguridad de la Aviación* (Doc 10108 – Distribución limitada).
14. Las operaciones de los aeropuertos en este contexto incluyen todos los servicios aeroportuarios necesarios para la llegada, salida y rodaje de aeronaves, así como la gestión del público pasajero, incluidos, entre otros, el acceso a las puertas de embarque, la disponibilidad de servicios de seguridad, la inspección de pistas, la gestión de equipajes, el combustible, el deshielo, el servicio de abastecimiento, la iluminación del aeropuerto y otros servicios relacionados.
15. En este contexto, las operaciones de las líneas aéreas incluyen todos los aspectos que repercuten en la capacidad de operar eficazmente una aeronave, incluida la información a la tripulación de vuelo, el mantenimiento de la aeronave, las operaciones de la aeronave, MET, la disponibilidad del GNSS frente a la navegación y la aproximación que no son de precisión, la información aeronáutica, etc.

MEDIO **Puntuación = 3**	**Grave:** - Lesiones a las personas - Incidente grave - Una reducción en la capacidad del personal de operaciones para hacer frente a condiciones operacionales adversas por el aumento en la carga de trabajo o por condiciones que afectan su eficiencia.	- Decenas de personas fallecidas - Cientos de millones de dólares estadounidenses - Perturbación apreciable del servicio y de la confianza en el sistema de aviación	- Interrupciones notables en la capacidad y/o eficiencia de la navegación aérea. - Interrupciones parciales o mal funcionamiento de sistemas operacionales clave, que afectan a múltiples servicios. - Retrasos moderados en la afluencia del tránsito aéreo o repercusión moderada en las operaciones aeroportuarias o de las líneas aéreas, lo que exige coordinación y recursos adicionales para su gestión.
MEDIO-BAJO **Puntuación = 2**	**Menor:** - Molestias y limitaciones operacionales - Uso de procedimientos de emergencia - Incidente leve	- Algunos de los impactos de las consecuencias del nivel MEDIO, pero no todos	- Interrupciones menores en la capacidad y/o eficiencia de la navegación aérea. - Incidente limitado que afecta a sistemas o servicios específicos. - Ligeros retrasos o ineficiencias en la afluencia del tránsito aéreo o en las operaciones aeroportuarias o de las líneas aéreas, manejables dentro de los procedimientos operacionales normales.
BAJO **Puntuación = 1**	**Insignificante:** - Posiblemente algunas lesiones - Pocas consecuencias	- Posiblemente algunas muertes y lesiones - Algún tipo de repercusión económica - Alguna perturbación del servicio y de la confianza en el sistema de aviación	- Interrupción mínima en la capacidad y/o eficiencia de la navegación aérea. - Incidente aislado con un impacto muy limitado en las operaciones generales. - Retrasos o interrupciones muy limitados en la afluencia del tránsito aéreo, repercusión muy limitada en las operaciones aeroportuarias o de las aerolíneas.

Vulnerabilidad

2.3.9 La vulnerabilidad se mide de forma cualitativa y describe la eficacia de las medidas existentes para mitigar las consecuencias de la hipótesis de una ciberamenaza en los activos afectados.

2.3.10 La evaluación de la vulnerabilidad debería realizarse en colaboración entre personas expertas en aviación y ciberespecialistas que puedan analizar la función crítica de la aviación en cuestión y evaluar la manera en que los actores de amenazas pueden explotar las vulnerabilidades cibernéticas.

Tabla 3. Clasificación de la vulnerabilidad de la ciberamenaza

CALIFICACIÓN DE VULNERABILIDAD		
ALTA	1	No hay medidas de mitigación vigentes, ya sea por la ausencia de requisitos o porque no se han implementado medidas efectivas reales.
MEDIA-ALTA	0,8	Las medidas de mitigación tienen un alcance limitado y las áreas y aspectos importantes del riesgo no están previstos en los requisitos o medidas vigentes.
MEDIA	0,6	Están presentes características de los niveles MEDIO-ALTO y MEDIO-BAJO.
MEDIA-BAJA	0,4	Por lo general, existen medidas de mitigación, pero puede que aún no hayan alcanzado madurez o que sean solo parcialmente efectivas. Por ejemplo, los manuales de seguridad de la información elaborados por la OACI pueden abarcar todas las esferas y aspectos, pero en la práctica podrían mejorarse o aplicarse mejor.
BAJA	0,2	Existen disposiciones claras y se están utilizando ampliamente medidas de mitigación que generalmente se consideran efectivas.

Ejemplo de evaluación de un ciberriesgo

Tabla 4. Matrices de evaluación y puntuación de ciberriesgos

MATRIZ DE EVALUACIÓN DE CIBERRIESGOS				
Hipótesis de ciberamenaza	**Probabilidad** **X**	**Impacto** **X**	**Vulnerabilidad**	**Riesgo residual** **=**
Un actor de amenazas utiliza un ciberataque para afectar a un activo de aviación gestionado por una parte interesada de la aviación en el que se explota una vulnerabilidad.	**MEDIA** **3**	**MEDIO-ALTO** **4**	**MEDIA-ALTA** **0,8**	**9,6**

MATRIZ DE PUNTUACIÓN DE CIBERRIESGOS	
PUNTUACIÓN DEL RIESGO	**CALIFICACIÓN DEL RIESGO**
20–25	ALTO
15–20	MEDIO-ALTO
10–15	MEDIO
5–10	MEDIO-BAJO
0–5	BAJO

APÉNDICES

Apéndice A

EJEMPLO DE APLICACIÓN DE LA METODOLOGÍA EN LA GESTIÓN DE RIESGOS PARA LA SEGURIDAD OPERACIONAL DE LA AVIACIÓN

SUPUESTOS Y DESCRIPCIÓN GENERAL

Este ejemplo ilustra la integración de la evaluación de los riesgos cibernéticos en la evaluación de los riesgos para la seguridad operacional de la aviación, utilizando una amenaza hipotética evaluada por un proveedor de servicios de navegación aérea (ANSP).

Supuestos:

- El ANSP ya ha valorado, evaluado y mitigado los riesgos de seguridad operacional pertinentes mediante el análisis de árbol de fallas (FTA)[16].
- Especialistas en seguridad operacional determinaron que el control de la comunicación aeroterrestre es una función crítica de la aviación.
- A efectos de simplificación, se supone que la ciberamenaza que se está evaluando solo afecta a la seguridad operacional (no repercute en la seguridad de la aviación, la eficiencia y/o la capacidad de la navegación aérea).
- El ANSP utiliza las mismas tablas de puntuación de probabilidad, impacto y vulnerabilidad que las empleadas en este documento.
- En la puntuación utilizada para la evaluación del ciberriesgo se usan valores diferentes a los del párrafo 3.3.17, ya que el alcance de la evaluación de este ejemplo se limita a los sistemas terrestres y a los datos relacionados con las CPDLC.
- Para simplificar, en la siguiente hipótesis de ciberamenaza, que se ilustra en la figura 3, se supone que la ciberamenaza solo repercute en los mensajes CPDLC relacionados con la autorización de nivel de vuelo.

Hipótesis de ciberamenaza:

- Las personas expertas en seguridad operacional trabajaron con ciberespecialistas para examinar las evaluaciones de riesgos de seguridad operacional existentes para la función de comunicaciones aeroterrestres e identificaron las CPDLC como sistema e información de apoyo a la función crítica que es necesario evaluar para determinar si presenta ciberriesgos.
- Las personas expertas en seguridad operacional plantearon una evaluación de riesgos existente de seguridad operacional para un suceso de seguridad principal relativo a las CPDLC: "Entrega espuria no detectada de uno o varios mensajes utilizados para dar autorizaciones (nivel de vuelo autorizado - CFL, dirección y velocidad) a una o varias aeronaves".
- Las personas ciberespecialistas, en análisis conjunto con personas expertas en seguridad operacional, determinaron que "la manipulación de datos de un mensaje CPDLC enviado por una controladora o un

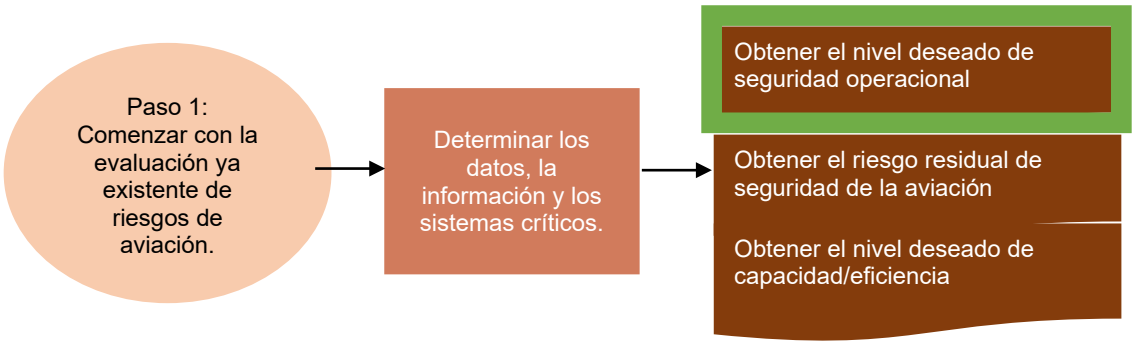
16. El FTA es una herramienta que ayuda a identificar y analizar las condiciones y los factores que causan, o contribuyen a que se produzca, un suceso no deseado definido, que por lo general afecta considerablemente la seguridad operacional, la actuación, la economía u otras características necesarias del sistema. El FTA se aplica intensivamente a la evaluación de la seguridad operacional de los sistemas.
La parte IV de la herramienta de metodología de evaluación electrónica de la seguridad operacional (eSAM) de EUROCONTROL (https://www.eurocontrol.int/tool/safety-assessment-methodology), anexo K, Fault Tree Analysis Guidance Material (textos de orientación sobre el análisis del árbol de fallas), contiene orientación sobre el uso del FTA.

controlador de tránsito aéreo a una pilota o un piloto" era una hipótesis de ciberamenaza que debe evaluarse e integrarse en la evaluación de riesgos de seguridad operacional ya mencionada.

- La hipótesis que se evalúa en este ejemplo se refiere a la manipulación deliberada de datos de un mensaje CPDLC, en la que un actor malicioso manipula un mensaje original (autorización de nivel de vuelo) enviado por una controladora o un controlador de tránsito aéreo a una pilota o un piloto (lo sustituye por un nivel de vuelo deliberadamente falso) antes de que se transmita a la aeronave.
- Para simplificar, el vector de ataque considerado se encuentra exclusivamente en el segmento terrestre de la infraestructura CPDLC: instalaciones en tierra del ANSP (red o servidores internos) o la red tierra-tierra del proveedor de servicios de comunicaciones o la red y servidores locales de la estación aeroterrestre, es decir, el ejemplo excluye otros vectores de ataque como la comunicación aeroterrestre de mensajes CPDLC. Utilizando el ejemplo de categorización de ciberamenazas del apéndice C (véase la versión de distribución limitada de este documento), esta ciberamenaza puede clasificarse como:
    - Dominio: proveedor de servicios de navegación aérea.
    - Función: comunicaciones, navegación, vigilancia (CNS).
    - Subfunción: comunicaciones.
    - Ciberamenaza: alteración (modificación del contenido del mensaje).

Figura 3. Amenaza: manipulación deliberada de datos
(Nota: Figura 4 en la versión de distribución limitada)

APLICACIÓN PASO A PASO DE LA METODOLOGÍA



- ⇨ Las personas expertas en seguridad operacional trabajaron con ciberespecialistas para examinar las evaluaciones de riesgos de seguridad operacional existentes para la función de comunicaciones aeroterrestres e identificaron las CPDLC como sistema e información de apoyo a la función crítica que es necesario evaluar para determinar si presenta ciberriesgos.
- ⇨ Las personas expertas en seguridad operacional elaboraron el diagrama original del árbol de fallas de seguridad operacional, sin causas de ciberriesgos[17]. El suceso principal relacionado con nuestra hipótesis de ciberamenaza a las CPDLC es: "un envío espurio no detectado de uno o varios mensajes utilizados para dar autorizaciones a una o varias aeronaves".
- ⇨ **El nivel de seguridad operacional deseado para el suceso principal es "no más de 10^-5 sucesos por hora de vuelo".**

17. Acrónimos del diagrama de árbol de fallas:

- AGDP: procesador de enlace aeroterrestre de datos, servidor de datos aeroterrestres CFL: nivel de vuelo autorizado
- CWP: puesto de trabajo de controlador/a (interfaz humano-máquina)
- FDPS: sistema de procesamiento de datos de vuelo

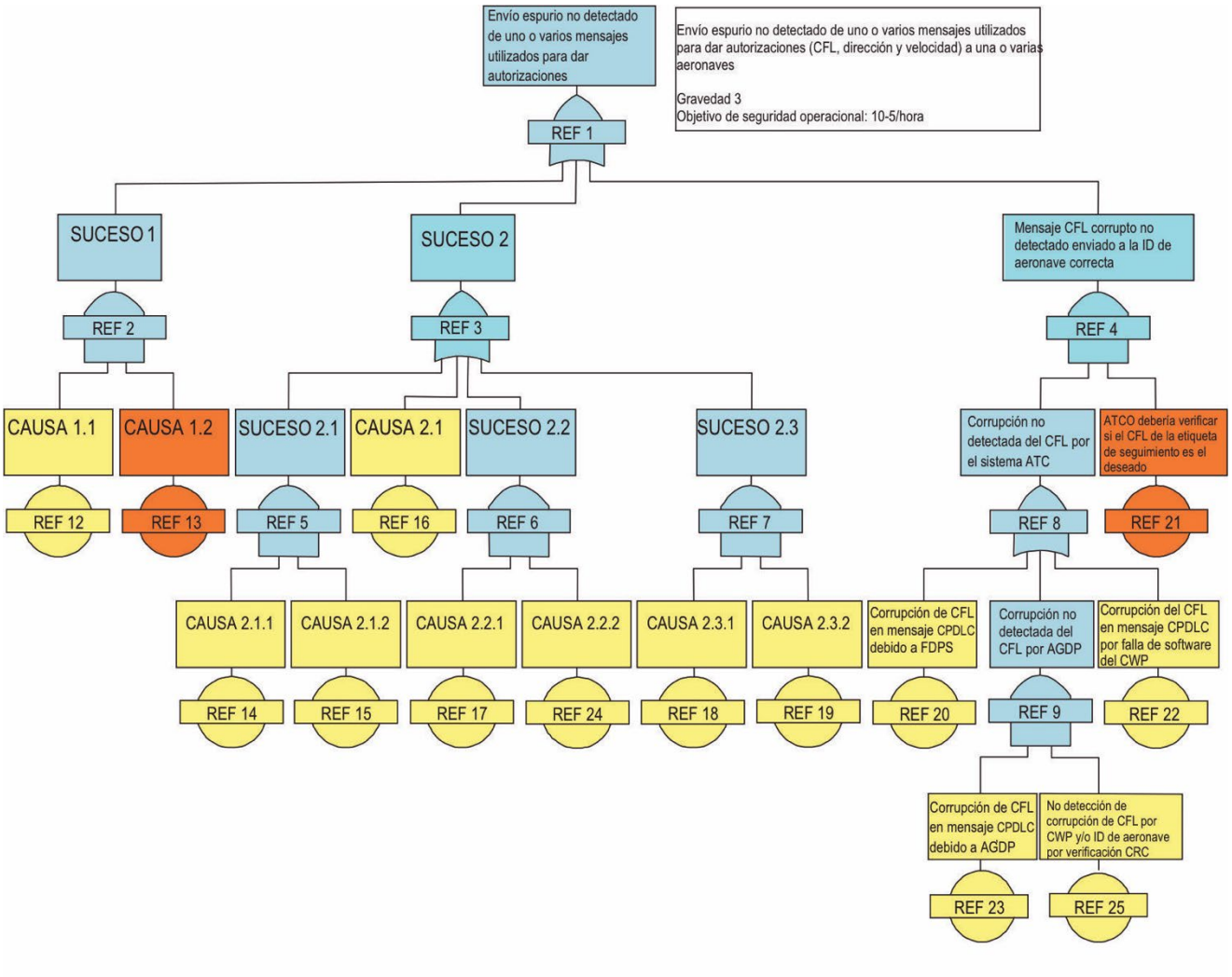
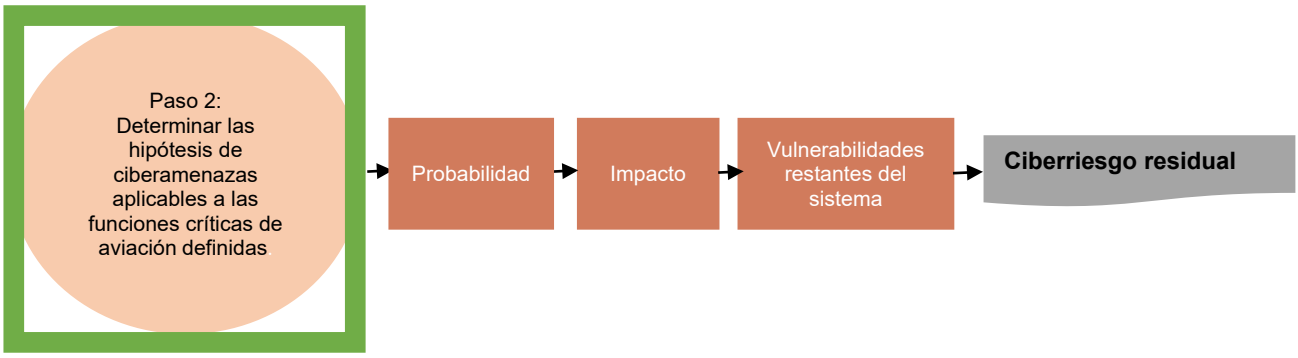


Figura 4. Diagrama de árbol de fallas original
(Nota: Figura 5 en la versión de distribución limitada)



- ⇨ Las personas ciberespecialistas, en análisis conjunto con personas expertas en seguridad operacional, determinaron que "la manipulación de datos de un mensaje CPDLC enviado por una controladora o un controlador de tránsito aéreo a una pilota o un piloto" era una hipótesis plausible de ciberamenaza que debe evaluarse e integrarse en la evaluación de riesgos de seguridad operacional ya mencionada.
- ⇨ La evaluación de ciberriesgos estuvo a cargo de ciberespecialistas del ANSP en colaboración con personas expertas en seguridad operacional. Las personas ciberespecialistas conocen los métodos y vectores de ataque de las ciberamenazas, mientras que las personas expertas en seguridad operacional conocen la arquitectura del sistema.

A los componentes de la evaluación de ciberriesgos del paso 2 se añaden los siguientes pasos:

Se siguieron los pasos que se indican a continuación para construir la matriz de ciberriesgos:

- ⇨ **Probabilidad:**
  - Las personas expertas en seguridad operacional suelen utilizar probabilidades (como el número de incidentes por horas de vuelo). Además, cuando se utilizan árboles de fallas, a veces se utiliza la "distancia" desde el suceso principal del árbol de fallas para calcular la probabilidad (por ejemplo, cuanto más lejos del suceso principal, menor es la probabilidad de que afecte al suceso principal en el sentido de alterar el nivel de seguridad deseado). Por otro lado, las personas ciberespecialistas suelen emplear tablas de probabilidad con valores discretos (como la tabla 1 del capítulo 2). El objetivo de este trabajo conjunto entre especialistas es poner en común lo que se entiende por los *distintos componentes del riesgo*.
  - Así, en este ejemplo, la inserción de la ciberamenaza en el árbol de fallas (los elementos en rojo) facilita la estimación de la probabilidad en términos de capacidad e intención de que la ciberamenaza se materialice[18].

18. En una evaluación completa del ciberriesgo, pueden añadirse numerosos vectores de ataque al diagrama original. En aras de la simplificación, el ejemplo incluye solo dos posibles vectores de ataque.

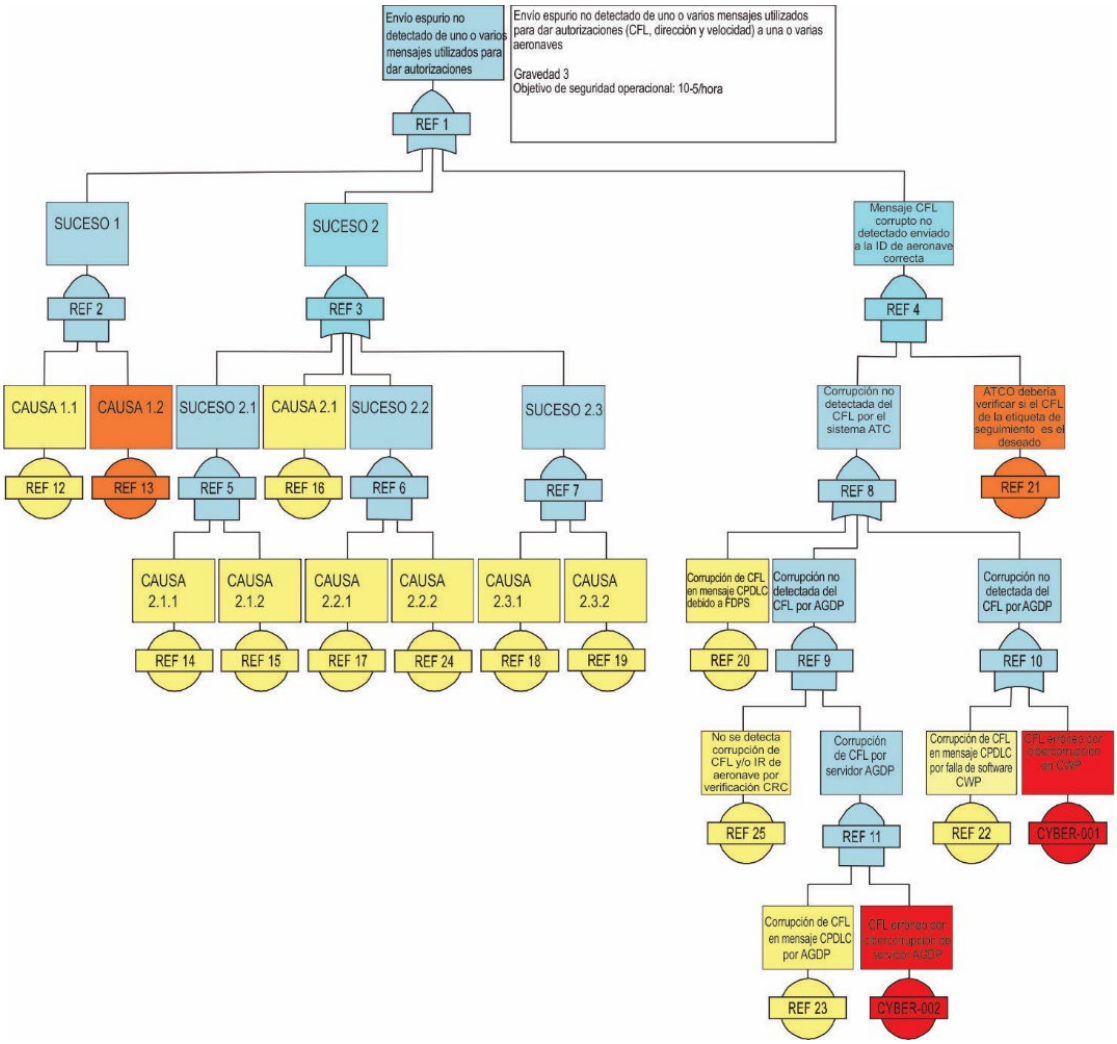


Figura 5. Diagrama de árbol de fallas actualizado
(Nota: Figura 6 en la versión de distribución limitada)

- Se asignó a la probabilidad de la ciberamenaza una puntuación de 2, que corresponde a un nivel MEDIO-BAJO (es decir, una hipótesis respecto de la cual no hay antecedentes o los hay pero no son recientes, pero sí existen indicios de intención, aunque con un método que aparentemente no está lo bastante desarrollado para una hipótesis de ataque certero o que es probable que se remplace por otras formas de ataque).

⇨ **Impacto/Consecuencia/Efecto:**

- Evaluar el impacto implica valorar la peor hipótesis que sea razonable, que en este caso significa que el ciberataque tuvo éxito y que no se pudo evitar el suceso principal. Así, la evaluación de impacto supone la mayor gravedad posible del suceso principal antes de la introducción de la ciberamenaza, que corresponde a un nivel de impacto MEDIO (impacto grave en la seguridad operacional: incidente grave con reducción de la capacidad del personal de operaciones para hacer frente a condiciones operacionales adversas por un aumento en la carga de trabajo o condiciones que afectan su eficiencia).

⇨ **Vulnerabilidad:**

- La evaluación de la vulnerabilidad se realiza teniendo en cuenta las medidas de mitigación existentes.
- A este respecto, el FTA indica que se realiza una verificación por redundancia cíclica (CRC) del mensaje CPDLC[19]. Así, se lo tiene en cuenta al igual que las medidas relacionadas con la seguridad informática (protección de sistemas y servidores) y la seguridad de la aviación (verificación de antecedentes y control de acceso).

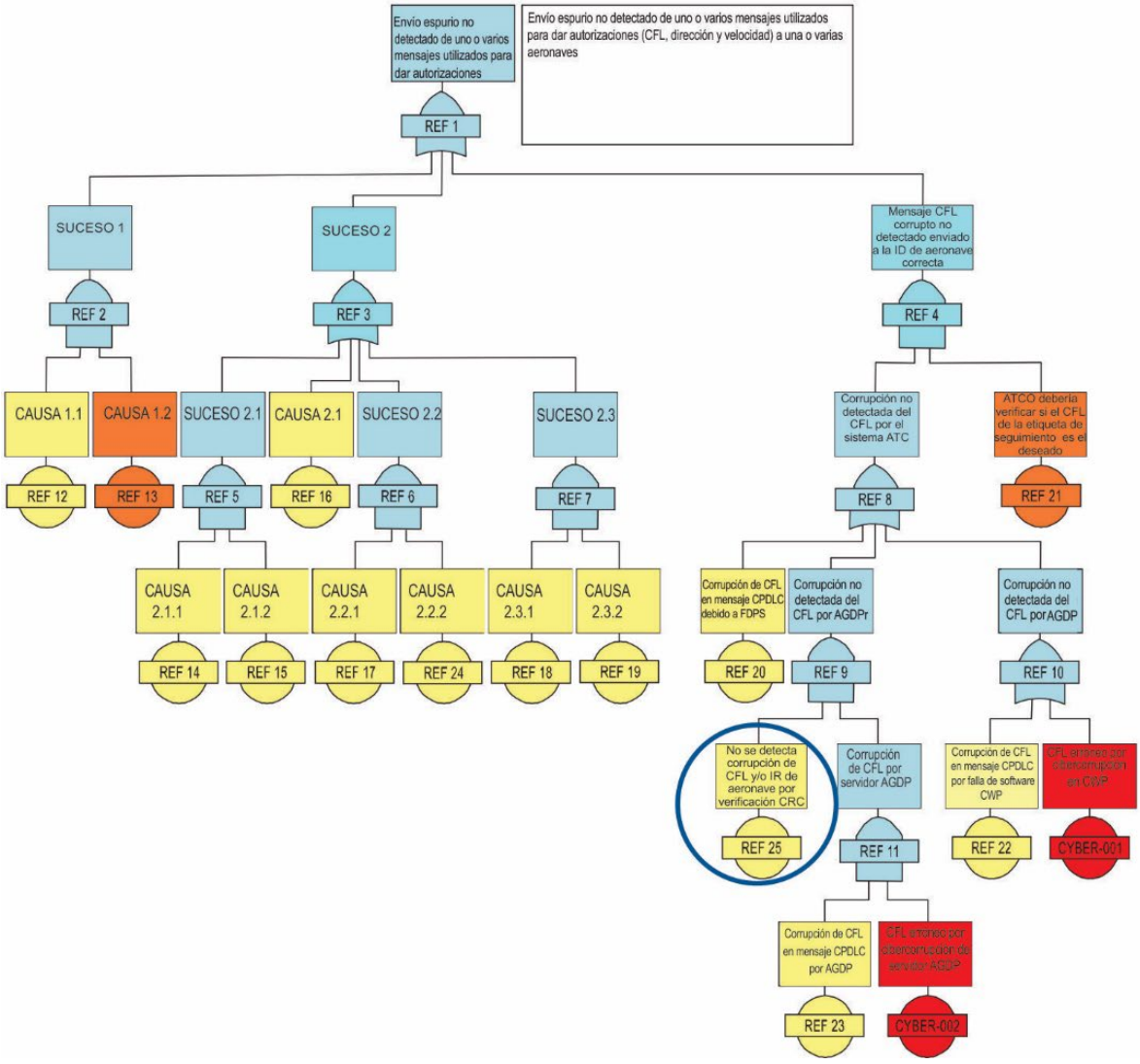


Figura 6. Diagrama de árbol de fallas actualizado (con círculo)

19. La *CRC* es un método para verificar que los datos no fueron alterados tras ser enviados en una comunicación. Fuente: NIST SP800-72

(Nota: Figura 7 en la versión de distribución limitada)

- Las personas ciberespecialistas son conscientes de que la CRC se utiliza principalmente para detectar errores involuntarios en los datos. No es efectiva para detectar interferencias intencionadas, ya que el atacante es capaz de cambiar el hash CRC al cambiar el mensaje y, por lo tanto, se concluye que los cibercontroles existentes podrían no bastar para mitigar el riesgo.
- Además, a partir de la evaluación de vulnerabilidades se concluyó que un ciberataque externo sería en cierto modo difícil de preparar y ejecutar. Las redes y sistemas de comunicación de los ANSP cuentan con protección adecuada contra ataques externos y la organización ha implementado capacidades adecuadas de monitoreo y detección. Sería relativamente más fácil organizar un ataque interno (amenaza interna), ya que las medidas de seguridad física aplicadas también son adecuadas (control de acceso a las salas pertinentes y verificación de los antecedentes del personal que tiene acceso a ellas).
- Por consiguiente, la vulnerabilidad recibe una puntuación MEDIA-ALTA (0,8).

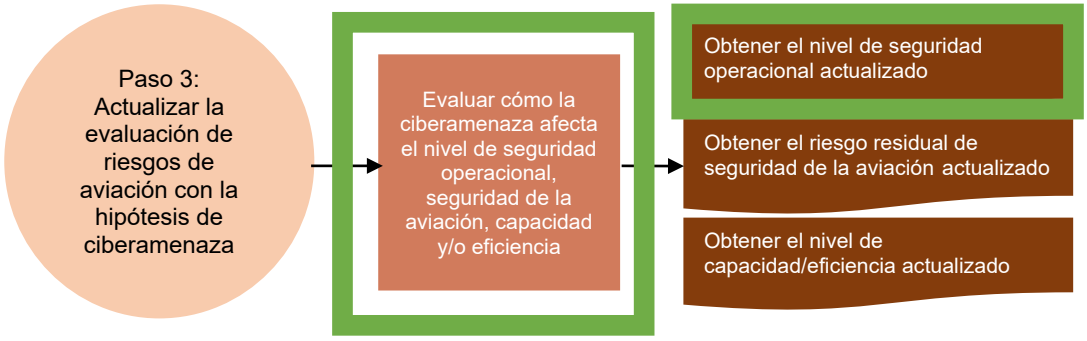
⇨ **Ciberriesgo residual:**

- Ahora se puede calcular el ciberriesgo residual multiplicando las puntuaciones de probabilidad, impacto y vulnerabilidad: **2 x 3 x 0,8 = 4,8.**

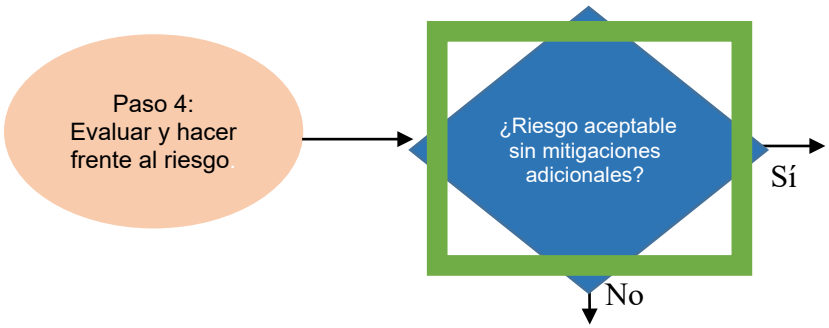
⇨ La puntuación del ciberriesgo residual de 4,8 se ha redondeado a 5, ya que las personas expertas lo consideraron más próximo a MEDIO-BAJO que a BAJO.

La matriz de ciberriesgo queda así:

MATRIZ DE CIBERRIESGO					
Hipótesis	**Probabilidad**	**Impacto**	**Mitigaciones**	**Vulnerabilidades**	**Riesgo residual**
Manipulación por un intruso de la carga útil de datos de un mensaje CPDLC enviado de una controladora o un controlador a una pilota o un piloto.	**Puntuación de 2** MEDIA-BAJA Hipótesis para la que no hay ejemplos, o no hay ejemplos recientes, pero existen ciertos indicios de intención, aunque con un método que aparentemente no está lo bastante desarrollado para una hipótesis de ataque certero o que es probable que se remplace por otras formas de ataque.	**Puntuación de 3** GRAVE Suceso principal de seguridad operacional: envío espurio no detectado de uno o varios mensajes utilizados para dar autorizaciones.	CRC Capacidades de monitoreo y detección de intrusos ya implementadas. Medidas de seguridad informática Control de acceso físico y verificación de antecedentes	**Puntuación de 0,8** MEDIA-ALTA La CRC no es una herramienta adecuada para detectar la manipulación maliciosa de la información, ya es posible manipularla junto con la información.	**Puntuación de 4.8 (redondeada a 5)** MEDIO-BAJO Esta puntuación se comparará con las puntuaciones de las demás hipótesis de amenaza y se utilizará para clasificar las amenazas.



- ⇨ Ahora que se ha actualizado el diagrama de árbol de fallas y que la organización tiene mucho más conocimiento sobre la ciberamenaza traducida en un ciberriesgo que corresponde a los objetivos de seguridad operacional, la evaluación original del riesgo de seguridad operacional se puede actualizar incluyendo la evaluación de la ciberamenaza, lo que podría arrojar una nueva probabilidad de ocurrencia del suceso principal de seguridad operacional (" envío espurio no detectado de uno o varios mensajes utilizados para dar autorizaciones").
- ⇨ Esto servirá de base para los siguientes pasos: evaluación y tratamiento del riesgo.

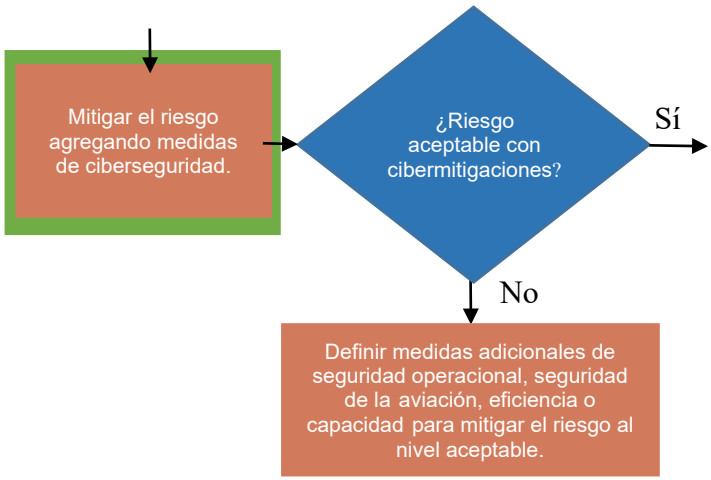


Con las evaluaciones actualizadas, el ANSP utiliza su matriz de aceptabilidad existente. Esta matriz de aceptabilidad puede contener distintos tipos de criterios, por ejemplo:

- Criterios cibernéticos, cuya fuente incluye reglamentos de aviación, reglamentos/leyes sobre infraestructura crítica, tolerancia de la organización al riesgo, etc.
- Criterios de seguridad operacional, que incluyen la relación entre el impacto en la seguridad operacional y la probabilidad de seguridad operacional deseada, así como fuentes relacionadas con los reglamentos de aviación pertinentes.
- Criterios de capacidad y eficiencia de la navegación aérea, que dependen de la organización (y no se contemplan en este ejemplo).

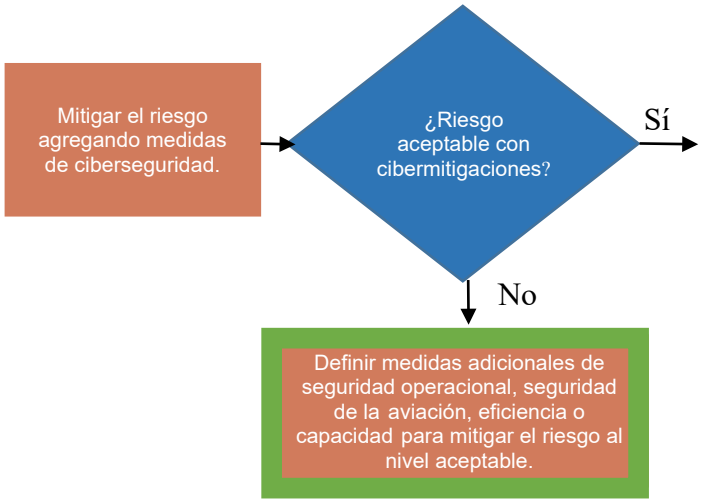
Esta evaluación con respecto a estos criterios de la organización debería dar lugar a una decisión: **¿Puede aceptarse el riesgo tal cual o deberían aplicarse medidas de cibermitigación que complementen los controles existentes?**

La evaluación llevó a la decisión de que, aunque el ciberriesgo residual es MEDIO-BAJO, debían considerarse medidas de mitigación adicionales para reducir aún más el riesgo.



⇨ **Medidas de mitigación de ciberseguridad:**

- Las personas ciberespecialistas propusieron en primer lugar incorporar nuevos equipos para proteger aún más el sistema de las interferencias. Sin embargo, las personas especialistas en seguridad operacional no estuvieron de acuerdo, ya que se crearían nuevos puntos de falla que requerirían examinar toda la evaluación de seguridad operacional del sistema, así como de otros sistemas afectados.
- Las personas expertas en seguridad operacional y ciberespecialistas coincidieron en que los controles establecidos para proteger el sistema contra un ciberataque externo son adecuados, por lo que decidieron centrarse en medidas para mitigar la amenaza interna, que se consideró más plausible durante la evaluación de ciberriesgos.
- Las segundas propusieron medidas para reforzar los privilegios de acceso a las computadoras y servidores pertinentes, que fueron aceptadas.



⇨ **Medidas de mitigación adicionales**

- Se determinó que, con estas medidas de mitigación de ciberseguridad, el riesgo puede reducirse aún más centrándose en otros tipos de medidas.
- Especialistas en seguridad de la aviación propusieron una verificación de antecedentes y medidas de control de acceso más estrictas para el personal autorizado a ingresar en el ATC y las salas de servidores.

- La evaluación del riesgo se repitió teniendo en cuenta las nuevas medidas (mitigaciones cibernéticas y de AVSEC) y se decidió que las nuevas medidas reducirían el riesgo a un nivel aceptable, por lo que se acordó su implementación.

⇨ **Matriz de ciberriesgo**

- Así, se completó la matriz de evaluación de ciberriesgos con medidas de mitigación adicionales que debían registrarse para su implementación, y la matriz final de evaluación de riesgos cibernéticos quedó del siguiente modo:

MATRIZ DE CIBERRIESGO						
Hipótesis	**Probabilidad**	**Impacto**	**Mitigaciones**	**Vulnerabilidades**	**Riesgo residual**	**Mitigaciones complementarias**
Manipulación por un intruso de la carga útil de datos de un mensaje CPDLC enviado de una controladora o un controlador a una pilota o un piloto.	**Puntuación de 2** MEDIO-BAJO Hipótesis para la que no hay ejemplos, o no hay ejemplos recientes, pero existen ciertos indicios de intención, aunque con un método que aparentemente no está lo bastante desarrollado para una hipótesis de ataque certero o que es probable que se remplace por otras formas de ataque.	**Puntuación de 3** GRAVE Suceso principal de seguridad operacional: envío espurio no detectado de uno o varios mensajes utilizados para dar autorizaciones.	CRC Capacidades de monitoreo y detección de intrusos ya implementadas. Medidas de seguridad informática Control de acceso físico/ verificación de antecedentes	**Puntuación de 0,8** MEDIA-ALTA La CRC no es una herramienta adecuada para detectar la manipulación maliciosa de la información, ya es posible manipularla junto con la información.	**Puntuación de 4.8 (redondeada a 5)** MEDIO-BAJO Esta puntuación se comparará con las puntuaciones de las demás hipótesis de amenaza y se utilizará para clasificar las amenazas.	**Cibermedidas: Optimización y monitoreo del privilegio de acceso digital en computadoras y servidores pertinentes.** **Otras medidas: verificación de antecedentes y medidas de control de acceso físico más estrictas para el personal autorizado a ingresar en el ATC y las salas de servidores.**

CONCLUSIÓN

El enfoque paso a paso de este ejemplo se ofrece a título ilustrativo para mostrar cómo deben interactuar las evaluaciones de seguridad operacional y de ciberriesgos para hacer frente a las amenazas y ciberriesgos para la aviación civil. En un entorno real, este proceso tendría lugar de forma más iterativa e integrada, según la estructura de gobernanza de la organización y de los marcos regulatorios o jurídicos vigentes.

Apéndice B

EJEMPLO DE APLICACIÓN DE LA METODOLOGÍA EN LA GESTIÓN DE RIESGOS PARA LA SEGURIDAD DE LA AVIACIÓN

SUPUESTOS Y DESCRIPCIÓN GENERAL

El ejemplo que figura a continuación ilustra la integración de la evaluación de ciberriesgos en la evaluación de riesgos para la seguridad de la aviación, utilizando una hipótesis de amenazas evaluada por un Estado.

Supuestos:

- El Estado ya ha evaluado, valorado y mitigado los riesgos pertinentes para la seguridad de la aviación utilizando matrices de riesgos de AVSEC.
- Las personas especialistas en seguridad de la aviación han definido la inspección del equipaje de mano como una función crítica de la aviación.
- A efectos de simplificación, se supone que la ciberamenaza que se está evaluando solo afecta a la seguridad de la aviación (y no a la seguridad operacional, la eficiencia y/o la capacidad de la navegación aérea).
- El Estado usa las mismas tablas de puntuación de probabilidad, impacto y vulnerabilidad que las utilizadas en este documento.
- En aras de la uniformidad, la puntuación utilizada en la evaluación de ciberriesgos se basa en los mismos valores que los del capítulo 3 de la versión de distribución limitada de este documento. Sin embargo, en realidad, las puntuaciones de probabilidad, impacto y vulnerabilidad de cada Estado y organización variarán según las diferentes variables que afecten estas calificaciones (capacidades, intención, medidas de mitigación existentes, etc.).
- Habida cuenta de la sensibilidad de las evaluaciones de riesgos para la seguridad de la aviación, solo se describe el proceso para integrar la evaluación de ciberriesgos en la evaluación de la seguridad de la aviación. El proceso de evaluación de ciberriesgos se describe en detalle.

Hipótesis de ciberamenazas:

- El Estado está analizando las distintas formas de proceder de un adversario que intenta llevar a bordo de una aeronave artefactos explosivos improvisados que una persona lleva ocultos (PBIED) en el equipaje de mano con la intención de derribar la aeronave.
- Las personas especialistas en seguridad de la aviación trabajaron con ciberespecialistas para examinar las evaluaciones existentes de los riesgos de AVSEC para la inspección del equipaje de mano y determinaron que el componente de detección del equipo de inspección constituía un sistema e información críticos (que respaldan la función crítica de aviación) que deben evaluarse para determinar si plantean un ciberriesgo.
- Las personas especialistas en seguridad de la aviación han elaborado una evaluación de los riesgos existentes de la seguridad de la aviación para los PBIED (en el cuerpo de la persona o en su equipaje de mano) y solo han considerado este último para el ejercicio de evaluación.
- En conversaciones con especialistas en seguridad de la aviación, las personas ciberespecialistas han definido “la manipulación de datos del componente de detección con el objetivo de alterar los resultados del proceso de inspección automatizado” como una hipótesis de ciberamenaza que debe evaluarse e integrarse en la evaluación de riesgos de seguridad de la aviación mencionada.
- Vector de ataque: este ataque podría llevarse a cabo interfiriendo con las capacidades de detección de los equipos mediante el acceso físico o remoto al equipo en cuestión.

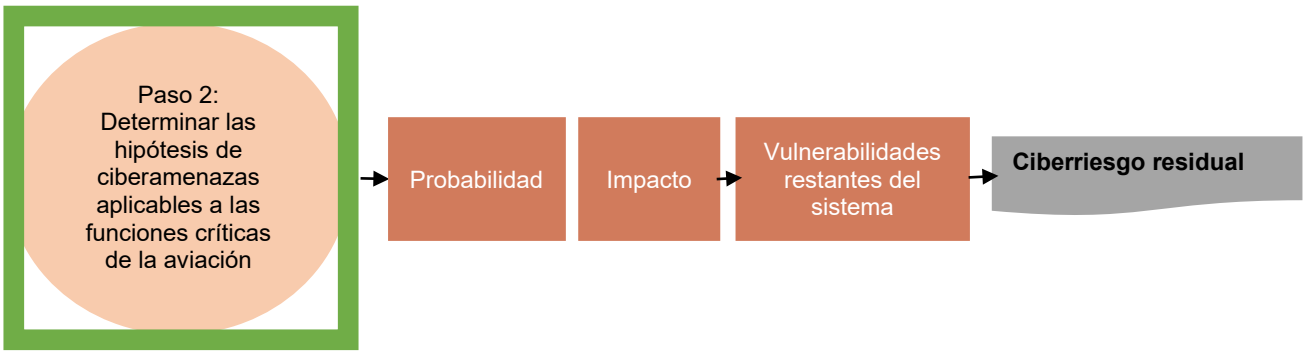
- Usando el ejemplo para la categorización de ciberamenazas que figura en el apéndice C (véase la versión de distribución limitada de este documento), esta ciberamenaza puede clasificarse de la siguiente manera:
  - Dominio: Aeropuerto.
  - Función: Seguridad de la aviación.
  - Subfunción: Inspección de equipaje de mano.
  - Ciberamenaza: Alteración (interferencia con el software o los sistemas de detección).

APLICACIÓN PASO A PASO DE LA METODOLOGÍA

⇨ Las personas especialistas en seguridad de la aviación trabajaron con ciberespecialistas para examinar las evaluaciones de los riesgos que plantean los PBIED en el equipaje de mano para seguridad de la aviación y determinaron que el componente de la función de detección del equipo de inspección consistía en un sistema e información que respaldan la función crítica que se necesita evaluar para detectar ciberriesgos.

⇨ Las personas especialistas en seguridad de la aviación elaboraron la evaluación inicial de riesgos de los PBIED sin causas cibernéticas. La hipótesis de seguridad de la aviación relacionada con nuestra hipótesis de ciberamenaza es: “una persona pasajera lleva a bordo un artículo prohibido con la intención de derribar el avión”.

⇨ **El resultado del proceso es obtener el riesgo residual para la seguridad de la aviación que supone la hipótesis presentada.**



⇨ Las personas ciberespecialistas, en colaboración con los especialistas en seguridad de la aviación, definieron “la manipulación de datos del componente de detección con el objetivo de alterar los resultados del proceso de inspección” como una hipótesis de ciberamenaza plausible que debe evaluarse e integrarse en la evaluación de riesgos para la seguridad de la aviación ya mencionada.

⇨ La evaluación de los ciberriesgos estuvo a cargo de ciberespecialistas del Estado en colaboración con especialistas en seguridad de la aviación. Las personas ciberespecialistas están familiarizadas con los métodos y los vectores de ataque cibernético conocidos, mientras que quienes se especializan en seguridad de la aviación conocen el equipo y sus niveles de tolerancia.

A los componentes de la evaluación de ciberriesgos del paso 2 se añaden los siguientes pasos:

Se aplicaron los siguientes pasos para evaluar los ciberriesgos en el ámbito de la seguridad de la aviación con el fin de crear la matriz de ciberriesgos:

⇨ **Probabilidad:**
- Las personas especialistas en seguridad de la aviación y las ciberespecialistas suelen usar tablas de probabilidad con valores discretos (como la tabla 1 del capítulo 2), para poner en común lo que se entiende por los diferentes componentes de riesgo.
- La capacidad de ejecutar el ciberataque que se está evaluando requeriría una preparación exhaustiva.
- Es difícil llevar a cabo un ataque externo, ya que el equipo de inspección es independiente (no está conectado a una red) o está conectado a una red cerrada local, y serían necesarios muchos conocimientos y esfuerzo para alterar el resultado del proceso de inspección.
- Una amenaza interna es posible, pero para alterar el resultado del proceso de inspección harían falta grandes esfuerzos y conocimientos, por ejemplo:
    - Conocimiento detallado del aeropuerto, puntos de inspección, horarios, etc.
    - Alto nivel de cooperación (el ataque no se puede llevar a cabo sin ayuda).
    - Acceso a las máquinas y/o a la red local.
- Existen indicios de intención.
- Así, se asignó a la probabilidad de la ciberamenaza una puntuación de 3, que es de nivel MEDIO (es decir, una hipótesis esencialmente plausible, con algún indicio de intención y capacidad y posiblemente algunos ejemplos).

⇨ **Impacto/consecuencia/efecto:**
- Evaluar el impacto implica valorar la peor hipótesis que sea razonable, que en este caso significa que el ciberataque fue exitoso.
- El resultado del ciberataque sería que el equipo de inspección diera un falso resultado e incluso no detectara elementos prohibidos. La consecuencia de esto podría ser la destrucción de la aeronave y cientos de muertes, posiblemente algunas en tierra. Otra consecuencia serían costos inmediatos muy elevados y daños económicos a largo plazo. Por lo tanto, el impacto sería ALTO (puntuación de 5).

⇨ **Vulnerabilidad:**
- La evaluación de la vulnerabilidad se lleva a cabo teniendo en cuenta las medidas de mitigación existentes.
- Con respecto a las mitigaciones existentes:
    - El Estado ha ordenado la aplicación de las normas y métodos recomendados (SARPS) del Anexo 17 – *Seguridad de la aviación* para la inspección de las personas pasajeras mediante sistemas de detección implementados por el aeropuerto.
    - El Estado también requiere que sus explotadores apliquen la norma 4.9.1 y el método recomendado 4.9.2 relacionados con el tratamiento de las ciberamenazas, por lo que el aeropuerto ha puesto en práctica las siguientes medidas:

- Existe una separación lógica 20 o física en las redes informáticas de la infraestructura comercial y operacional.
- Se verifican los antecedentes del personal y se implementan medidas de seguridad de la aviación para proteger el acceso al equipo.

- Las personas ciberespecialistas han confirmado que los controles ya implementados son satisfactorios para mitigar el ciberriesgo. Sin embargo, como los especialistas en seguridad de la aviación son conscientes de que los requisitos del aeropuerto no se aplican de manera uniforme en todo el mundo (especialmente aquellos relacionados con los métodos recomendados), se acordó clasificar la vulnerabilidad como MEDIA-BAJA (0,4).

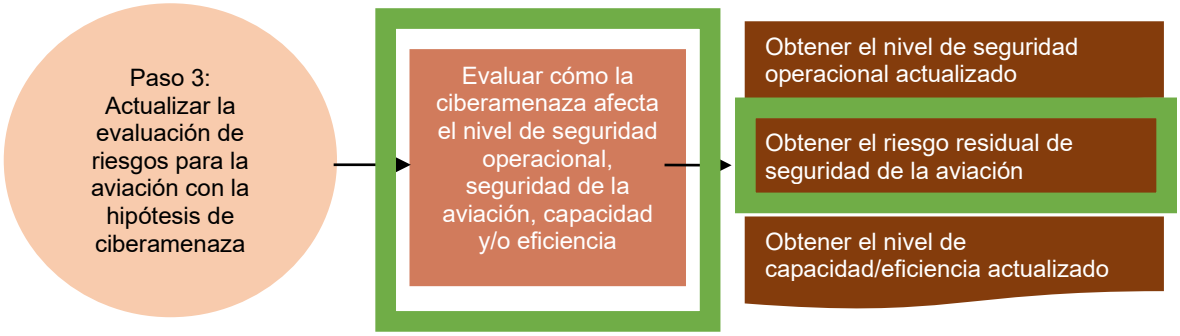
⇨ **Ciberriesgo residual:**

- El ciberriesgo residual se calcula multiplicando las puntuaciones de probabilidad, impacto y vulnerabilidad: 3 x 5 x 0,4 = 6, con lo que se obtiene un ciberriesgo residual MEDIO-BAJO.

La matriz de ciberriesgo queda así:

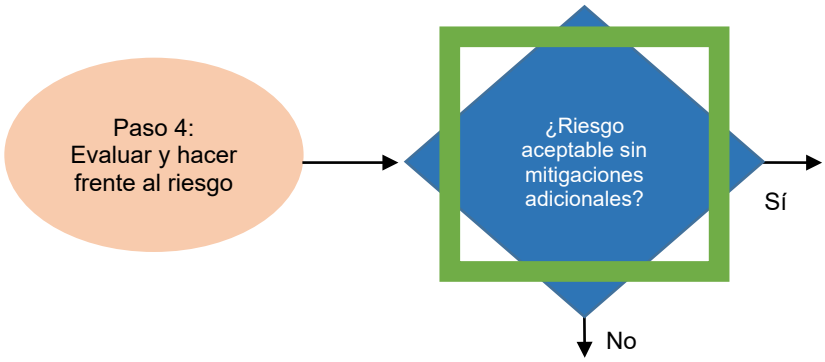
MATRIZ DE CIBERRIESGO					
Hipótesis	**Probabilidad**	**Impacto**	**Mitigaciones**	**Vulnerabilidades**	**Riesgo residual**
Una persona pasajera lleva a bordo un artículo prohibido con la intención de derribar el avión, alterando los resultados del equipo de inspección de seguridad.	**Puntuación de 3** MEDIA ¿Podría hacerlo un adversario? ¿Hay interés en atacar un blanco de aviación civil?	**Puntuación de 5** ALTO En la peor de las hipótesis razonables: ¿cuántas vidas se perderán? ¿Se esperan daños a la infraestructura? ¿Perderá el público la con-fianza en el transporte aéreo? ¿Cuál es el costo económico?	La norma 4.9.1 y el método recomendado 4.9.2 del Anexo 17 se aplican a la inspección de personas pasajeras mediante sistemas de detección.	**Puntuación de 0,4** MEDIA-BAJA Tras examinar las medidas de mitigación actuales, ¿qué tan vulnerable es la aviación ante esta hipótesis de amenaza?	**Puntuación de 6** La puntuación se comparará con las otras puntuaciones de hipótesis de amenazas y se usará para clasificar las amenazas.

20. La *separación lógica* se refiere a la segmentación de la red mediante la creación de zonas lógicas (virtuales) en la misma red física o *hardware*.



- Una vez que la ciberamenaza se traduce en un ciberriesgo que se alinea con los objetivos de seguridad de la aviación, la evaluación inicial del riesgo para la seguridad de la aviación puede actualizarse, incluida la evaluación de la ciberamenaza, que ahora se integra a la matriz de riesgos para la seguridad de la aviación para la hipótesis en cuestión, lo que podría dar lugar a un nuevo riesgo residual para la seguridad de la aviación.

- Esto servirá de base para los próximos pasos: evaluación de riesgos y respuesta.



- Con los datos, el Estado actualizará su matriz de riesgos PBIED e incluirá este *modus operandi*.

La evaluación debería dar lugar a una decisión: **¿Se puede aceptar el riesgo tal cual, o deberían aplicarse cibermitigaciones además de los controles actuales?**

- Se concluyó que el ciberriesgo residual era demasiado bajo para cambiar la evaluación original y, por lo tanto, el riesgo residual de la hipótesis general de amenaza de tipo PBIED no se ve afectado por esta hipótesis de ciberamenaza (es decir, la amenaza para la seguridad de la aviación permanece en el mismo nivel más elevado).
- Las personas ciberespecialistas también se mostraron satisfechas con los controles implementados para respaldar la integridad del proceso de inspección.
- Sin embargo, señalaron que cualquier cambio que se efectúe al equipo requiere la recertificación por parte de la autoridad pertinente, lo que puede exponer el sistema a futuras ciberamenazas si las vulnerabilidades descubiertas no se pueden rectificar oportunamente. Por ende, se ha iniciado un proyecto para encontrar un enfoque equilibrado entre la certificación y la actualización de los controles de ciberseguridad en los equipos de inspección, cuyo resultado se ha registrado como medida de mitigación adicional para su implementación futura para la mitigación del ciberriesgo.
- Por lo tanto, la matriz de ciberriesgo actualizada para esta hipótesis es la que figura a continuación.

MATRIZ DE CIBERRIESGO						
Hipótesis	**Probabilidad**	**Impacto**	**Mitigaciones**	**Vulnerabilidades**	**Riesgo residual**	**Mitigaciones suplementarias**
Una persona pasajera lleva a bordo un artículo prohibido con la intención de derribar el avión, alterando los resultados del equipo de inspección de seguridad.	**Puntuación de 3** MEDIO ¿Podría hacerlo un adversario? ¿Hay interés en atacar un blanco de aviación civil?	**Puntuación de 5** ALTO En el peor de los casos: ¿cuántas vidas se perderán? ¿Se esperan daños a la infraestructura? ¿Perderá el público la confianza en el transporte aéreo? ¿Cuál es el costo económico?	La norma 4.9.1 y el método recomendado 4.9.2 del Anexo 17 se aplican a la inspección de personas pasajeras mediante sistemas de detección.	**Puntuación de 0,4** MEDIO-BAJO Tras examinar las medidas de mitigación actuales, ¿qué tan vulnerable es la aviación ante esta hipótesis de amenaza?	**Puntuación de 6** La puntuación se comparará con las otras puntuaciones de hipótesis de amenazas y se usará para abordar las amenazas.	Elaboración de procesos para equilibrar la aplicación de parches a las vulnerabilidades y la recertificación de equipos de inspección de equipaje de mano.

CONCLUSIÓN

El enfoque paso a paso de este ejemplo se proporciona a fines ilustrativos para mostrar cómo deben interactuar las evaluaciones de seguridad de la aviación y de los ciberriesgos a fin de dar respuesta a las ciberamenazas y ciberriesgos para la aviación civil. En una situación real, el proceso se llevaría a cabo de manera más iterativa e integrada, según la estructura de gobernanza del Estado o de la organización y de los marcos reglamentarios o jurídicos en vigor.

— FIN —

ISBN 978-92-9275-970-4