OACI

SECURITY AND FACILITATION

Intercambio de Ciberinformación

Publicado bajo la responsabilidad del Secretario General
2024,Versión 1

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

Índice

ACRÓNIMOS

ANSP	Proveedores de servicios de navegación aérea
CAA	Administración de Aviación Civil
CERT	Equipo de Respuesta a Emergencias Informáticas
CIShP	Política de Intercambio de Ciberinformación;
CSIRT	Equipo de Respuesta a Incidentes de Ciberseguridad
CTI	Inteligencia sobre ciberamenazas
FIRST	*Forum of Incident Response and Security Teams* [Foro de equipos de seguridad y respuesta a incidentes]
OACI	Organización de Aviación Civil Internacional
IoC	Indicadores de Compromiso
IPR	Derechos de propiedad intelectual
ISAC	Centro de Intercambio y Análisis de Información
ISMS	Sistema de Gestión de la Seguridad de la Información
IT	Tecnología de la Información
OSINF	Información de Fuentes Abiertas
OSINT	Inteligencia de Fuentes Abiertas
SOC	Centro de Operaciones de Seguridad
TLP	Protocolo de Luces de Semáforo
TTP	Tácticas, Técnicas y Procedimientos
UAS	Sistema(s) de Aeronaves No Tripuladas

RESUMEN

Las mejores prácticas establecidas en materia de seguridad operacional y de seguridad de la aviación demuestran la importancia del intercambio de información y su papel en la reducción de las amenazas y los riesgos para la aviación civil. El intercambio de ciberinformación es igualmente importante.

El intercambio de ciberinformación es crucial para la gestión de los ciberriesgos en la aviación civil. Fomenta una sólida cultura de ciberseguridad, ya que promueve la colaboración y la confianza. También contribuye a la conciencia de la situación, la gestión operacional y táctica de los ciberriesgos y la planificación estratégica.

Este documento proporciona orientaciones a los Estados y a las partes interesadas del sector para la elaboración de un plan destinado a compartir ciberinformación, e incluye recomendaciones sobre el establecimiento de políticas, recursos y pasos a seguir para la aplicación y mejora continua de las prácticas de intercambio.

También se describen los prerrequisitos necesarios para compartir ciberinformación en el sector de la aviación. Se enumeran varios tipos de ciberinformación que se pueden compartir. También se evalúan aspectos como el análisis y el aseguramiento del intercambio de ciberinformación, y se pone énfasis en la necesidad de evaluar la fiabilidad de la fuente y la credibilidad de la información.

Este documento reemplaza la guía de la OACI publicada anteriormente sobre el uso del Protocolo del Semáforo (TLP) en la aviación civil. Proporciona reglas para compartir ciberinformación en el sector de la aviación en función de la norma del TLP actualizada, el tipo de información que se desee compartir, la fecha/hora en que se comparta y los destinatarios (por ejemplo, organismos estatales, explotadores, proveedores de servicios).

En general, en el documento se destaca la importancia de compartir diversos tipos de ciberinformación en el sector de la aviación civil, teniendo en cuenta al mismo tiempo el análisis, el aseguramiento y el etiquetado adecuado de la información para su distribución efectiva entre las partes interesadas pertinentes.

Esta guía se ajusta a la Estrategia[1] de Ciberseguridad de la Aviación de la Organización de Aviación Civil Internacional (OACI) y su Plan de Acción[2] de Ciberseguridad, y responde a la necesidad de compartir ciberinformación. La información contenida en este documento responde a los principios generales de las orientaciones de la OACI sobre seguridad operacional e intercambio de información sobre seguridad de la aviación incluidos en el *Manual de seguridad de la aviación* (Doc 8973 – De distribución limitada) y el *Manual de gestión de la seguridad operacional* (Doc 9859).

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

DEFINICIONES

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

Aseguramiento. Acciones planificadas y sistemáticas necesarias para generar confianza suficiente en que un producto o proceso satisface determinados requisitos.

Autenticación. Medida diseñada para verificar la identidad de cualquier persona, usuario, programa, proceso, sistema o dispositivo.

Ciberactivo. Elementos digitales y físicos que tienen valor comercial o para las operaciones, la seguridad operacional, la protección, la eficiencia y/o la capacidad de la aviación, tales como: sistemas, información, datos, redes, dispositivos, programas o equipos informáticos, procesos, *firmware* (programas almacenados en la memoria no volátil y rutinas del procesador), personal pertinente/certificado y otros recursos electrónicos.

Ciberamenaza. Cualquier posible ciberevento susceptible de menoscabar 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. Cibersuceso o serie de cibersucesos que inciden negativamente en 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 activas las funciones críticas aun en condiciones adversas o estrés, y de recuperarse de esas condiciones adversas.

Ciberriesgo. Posibilidad de un resultado no deseado a raíz de un cibersuceso.

Ciberseguridad de la aviación. Conjunto de tecnologías, controles y medidas, procesos, procedimientos y prácticas diseñados para asegurar 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 sea divulgado o puesto a disposición de cualquier persona, usuario, programa, proceso, sistema o dispositivo no autorizado.

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

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

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.

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

Intercambio de información. Proceso a través del cual una entidad proporciona información a una o más entidades para facilitar la toma de decisiones en función el riesgo y promover las mejores prácticas.

Seguridad de la información. Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Vector de ataque. Medio de acceso utilizado por una persona atacante para iniciar un ataque.

1. INTRODUCCIÓN

1.1 Justificación del intercambio de ciberinformación

El intercambio de información es fundamental para la gestión de los ciberriesgos de la aviación. En el mundo interconectado de hoy, las ciberamenazas plantean riesgos significativos para el sector de la aviación civil. Los ciberataques pueden ir dirigidos a cualquier aspecto del sistema de aviación, desde los sistemas de gestión del tránsito aéreo hasta los sistemas de datos de pasajeras y pasajeros, lo que puede provocar la disrupción de las operaciones y poner en peligro la seguridad del pasaje. Por lo tanto, para una gestión eficaz del ciberriesgo, se requiere de un enfoque colaborativo que incluya el intercambio de información entre las partes interesadas.

Las enseñanzas extraídas de la gestión de la seguridad operacional y de la seguridad de la aviación indican que una cultura de intercambio de información reducirá considerablemente los riesgos que plantean para la aviación civil los agentes malintencionados. En el sector de la aviación, el intercambio de información ha demostrado ser un instrumento valioso para gestionar los riesgos, tanto de seguridad operacional como de seguridad de la aviación. El mismo principio se aplica a la ciberseguridad de la aviación. Compartir ciberinformación permite a las partes interesadas comprender mejor las ciberamenazas que enfrentan, detectar vulnerabilidades y tomar medidas adecuadas para prevenir o mitigar los ciberataques contra la aviación civil.

El intercambio de información es también un aspecto esencial de una cultura de ciberseguridad sólida. Una cultura de ciberseguridad sólida es fundamental para poder reconocer las ciberamenazas y darles una respuesta eficaz. El intercambio de información es una parte intrínseca de esa cultura, ya que promueve la transparencia, la colaboración y la confianza entre las partes interesadas. El intercambio efectivo de ciberinformación contribuye a que todas las partes interesadas tengan los insumos necesarios para tomar decisiones informadas y medidas apropiadas, mitigar las ciberamenazas y/o hacer frente a los ciberincidentes y recuperarse tras ellos.

Por ciberinformación no solo se entiende la información que permite tomar medidas concretas, sino cualquier tipo de inteligencia que pueda incidir en los ciberriesgos para la aviación civil. El intercambio de ciberinformación no se limita a la inteligencia referida específicamente a lo cibernético. Incluye cualquier información pertinente que pueda contribuir a individualizar y mitigar los ciberriesgos en el sector de la aviación civil. Por ejemplo, la información sobre violaciones de la seguridad física, amenazas internas, contexto geopolítico, tecnología o vulnerabilidades de la cadena de suministro también puede ayudar a las partes interesadas a comprender mejor las ciberamenazas y los ciberriesgos y así poder mitigarlos.

El intercambio de ciberinformación contribuye a lo siguiente:

- **Planificación estratégica** para desarrollar capacidades de ciberseguridad de la aviación. Al compartir información, las partes interesadas pueden detectar deficiencias en sus capacidades de ciberseguridad y desarrollar estrategias adecuadas para mejorar su ciberresiliencia. La planificación estratégica procura que el sector de la aviación permanezca protegido y resiliente ante las ciberamenazas, y que las partes interesadas estén preparadas para responder a posibles ciberincidentes y recuperarse de ellos.
- **Conciencia de la situación** tanto en operaciones diarias como durante un ciberincidente. El intercambio de ciberinformación permite a las partes interesadas comprender mejor su postura con respecto a la ciberseguridad, el panorama de ciberamenazas y las posibles vulnerabilidades (debilidades) en sus sistemas.

También les permite individualizar los riesgos potenciales y tomar las medidas adecuadas para prevenir o mitigar el impacto de los ciberincidentes.

- **Gestión operacional y táctica de los ciberriesgos** en previsión y respuesta a una ciberamenaza. Al compartir información, las partes interesadas pueden detectar ciberamenazas y desarrollar estrategias adecuadas de gestión de riesgos.
- **Gestión de crisis** durante un ciberincidente, instancia en la que el intercambio efectivo de información permite a las partes interesadas coordinar su respuesta y tomar las medidas adecuadas para mitigar el impacto de un incidente.

Es esencial reconocer que para que el intercambio de información sea efectivo, es fundamental que haya confianza entre quienes participan del intercambio. Esta guía tiene como objetivo contribuir a que se genere la confianza necesaria para alentar a un grupo de participantes a superar las dudas que es natural que tengan al compartir información. Para ello, es necesario establecer un conjunto de reglas y procedimientos comunes que todas las partes integrantes del grupo de intercambio entiendan, acepten y cumplan. Llegar a un consenso sobre qué ciberinformación se va a compartir, cómo se compartirá y mediante qué método de distribución facilitará el intercambio efectivo de información.

Esta guía complementa el trabajo holístico de la OACI en materia de ciberseguridad de la aviación. Contribuye al pilar 5 de la Estrategia de Ciberseguridad de la Aviación de la OACI, Intercambio de información, y forma parte de la acción CyAP 5.1 del Plan de Acción de Ciberseguridad, que consiste en que la OACI elabore orientación para el intercambio de ciberinformación.

Este documento incorpora y reemplaza el texto de orientación de la OACI publicado anteriormente sobre el uso del Protocolo de Luces de Semáforo (TLP) en la aviación civil. En el presente documento se incluyen orientaciones sobre cómo utilizar la versión 2.0 actualizada del Protocolo TLP[3], elaborada por FIRST [*Forum of Incident Response and Security Teams* (Foro de equipos de seguridad y respuesta a incidentes)], como medio para el intercambio de ciberinformación en la aviación civil.

1.2 Contexto del intercambio de ciberinformación

Antes de adentrarnos en el intercambio de ciberinformación, es necesario abordar el ciclo de vida general de la ciberinteligencia.

El ciclo de vida de la ciberinteligencia es un proceso reiterativo fundamental en el campo del análisis de inteligencia. Cada paso del ciclo cumple un propósito esencial para que la información se transforme a partir de datos sin procesar en inteligencia valiosa que puede servir para facilitar la toma de decisiones, mejorar la ciberseguridad y contribuir al logro de varios objetivos estratégicos de una organización.

El intercambio de información (también llamado “Difusión” en la Figura 1, a continuación) es parte del ciclo de vida de la ciberinteligencia, que incluye los siguientes pasos:

1. Planificación y dirección: El primer paso para recopilar y analizar ciberinformación consiste en planificar y dirigir el proceso. Esto implica definir los objetivos de la recopilación y el análisis, determinar su alcance y escala e identificar a las partes interesadas que necesitan participar. La planificación y la dirección también implican la elaboración de políticas y procedimientos para recopilar y analizar información, así como la definición de las funciones y responsabilidades de quienes participan en las diferentes etapas.

[3] https://www.first.org/tlp/

2. Recopilación: El segundo paso es la recopilación real de ciberinformación. Esto implica recopilar datos de diversas fuentes (véase la sección 3). Puede realizarse manualmente o mediante procesos automatizados. Es esencial asegurarse de que los datos recopilados sean pertinentes, exactos y oportunos.

3: Procesamiento: El tercer paso consiste en procesar la información recopilada. Esto implica convertir los datos recopilados a un formato utilizable, analizarlos y detectar secuencias o anomalías que puedan indicar que existe una ciberamenaza, por ejemplo. Para este paso pueden utilizarse herramientas de procesamiento de datos, algoritmos y otras técnicas de análisis para detectar posibles ciberamenazas o vulnerabilidades, por ejemplo. El procesamiento también implica determinar la importancia y urgencia de la información y priorizar la respuesta en consecuencia.

4. Análisis y producción: El cuarto paso consiste en analizar y elaborar informes en función de los datos procesados. Esto implica interpretar los datos, identificar secuencias o tendencias y determinar los ciberriesgos que existen en el sistema de aviación, por ejemplo. Este paso puede llevar a rechazar la información si la calidad y el nivel de detalle no son suficientes para poder analizarla. Quienes analizan los datos utilizan su conocimiento y experiencia para dar sentido a los datos y producir informes de inteligencia que sean relevantes para su público destinatario, exactos y que puedan dar lugar a acciones concretas. La etapa de análisis y producción también puede incluir la formulación de recomendaciones para mitigar o prevenir ciberamenazas, por ejemplo.

5. Difusión (intercambio de ciberinformación) y comentarios: El último paso consiste en difundir los informes de inteligencia a las partes interesadas pertinentes. Puede incluir el intercambio de ciberinformación con partes interesadas internas (por ejemplo, equipos de tecnología de la información (IT), equipos de ciberseguridad y/o equipos de seguridad operacional o de seguridad de la aviación), así como con partes interesadas externas (tales como otras organizaciones de aviación u organismos estatales). La difusión implica asegurarse de que la ciberinformación se comparta en forma oportuna y segura, y que las partes interesadas tengan el contexto y el conocimiento necesario para actuar en consecuencia. La difusión eficaz contribuye a crear una cultura de intercambio de ciberinformación en el sector de la aviación civil y permite a las partes interesadas tomar medidas adecuadas que podrían permitir, por ejemplo, prevenir o mitigar las ciberamenazas.

En este paso, también se recogen comentarios para evaluar la efectividad y relevancia del ciclo de vida de la ciberinteligencia con el objetivo de mejorarlo en futuras ocasiones.

Figura 1. Ciclo de vida de la ciberinteligencia

2. POLÍTICA DE INTERCAMBIO DE CIBERINFORMACIÓN (CIShP)

En esta sección se proporcionan orientaciones sobre cómo desarrollar e implementar una política de intercambio de ciberinformación entre organizaciones (por ejemplo, entre partes interesadas de la aviación).

Estas orientaciones también pueden ser útiles a los Estados para elaborar sus planes de intercambio de ciberinformación. Sin embargo, es importante señalar que los sistemas nacionales de intercambio de ciberinformación pueden ser intersectoriales y no específicos de la aviación.

2.1 Política de intercambio de ciberinformación (CIShP)

En la política, se debería definir:

- El motivo del intercambio de ciberinformación;
- El alcance de la aplicabilidad, el contexto y las limitaciones (por ejemplo, fuentes de ciberinformación, limitaciones relacionadas con los derechos de propiedad intelectual, leyes de privacidad);
- Miembros de la comunidad de intercambio de ciberinformación dentro de la organización y sus respectivas responsabilidades;
- Normas de distribución (incluida la distribución ulterior[4]) de la ciberinformación dentro y fuera de la organización en función de las normas de clasificación/categorización de la información y de los requisitos reglamentarios y jurídicos pertinentes;
- Procedimientos operacionales:
  - Recopilación de información;
  - Desidentificación, si es necesario;
  - Validación de contenidos; y
  - distribución; y
- Ciclo de examen de la política y control de documentación (es decir, registro de cambios significativos y procedimientos de validación).

La organización debería aprobar la política como parte del sistema de gestión de la seguridad de la información (ISMS)[5]. La política debería someterse a un examen periódico (por ejemplo, anualmente), después de cualquier cambio significativo o de cualquier ciberincidente para tener en cuenta lo aprendido.

2.2 Requisitos reglamentarios y contractuales[6]

La política debe cumplir con todas las reglamentaciones aplicables y los acuerdos existentes relacionados con el intercambio de ciberinformación, tales como:

- Normativa nacional, regional y/o internacional intersectorial.
- Normativa nacional, regional y/o internacional específica de la aviación.

[4] En la sección 5 de este documento, se describe con más detalle el intercambio de información.
[5] ISO 27001, capítulo A.5.14 *Transferencia de información*
[6] Puede encontrarse información adicional (intersectorial) en:

NIST.SP.800-150 – Guía para el intercambio de información sobre ciberamenazas (sólo disponible en inglés)
Intercambio de información de ciberseguridad de ENISA (Agencia de la Unión Europea para la Ciberseguridad): Resumen de los enfoques reglamentarios y no reglamentarios
https://digital-strategy.ec.europa.eu/es/policies/nis2-directive

- Acuerdos con centros nacionales o internacionales de intercambio y análisis de información (ISACs) y equipos de respuesta a emergencias informáticas/equipos de respuesta a incidentes de ciberseguridad (CERT/CSIRT) (por ejemplo, ISAC de aviación, equipo europeo de respuesta a emergencias informáticas de gestión del tránsito aéreo (EATM-CERT), CERT/CSIRT nacionales).

2.3 Recursos

La organización debería determinar los recursos necesarios para que la política se aplique adecuadamente, entre ellos:

- Recursos humanos: aprovechar los equipos de ciberseguridad existentes, como el equipo del Centro de Operaciones de Seguridad (SOC), y contratar a nuevas personas según sea necesario;
- Recursos técnicos: sitio web, correo electrónico, teléfono, mensajes de texto, así como plataformas de intercambio seguras y/o de confianza; y
- Recursos financieros: costos relacionados con la adquisición y/o desarrollo de sistemas, formación de recursos humanos, etc.

2.4 Aplicación

La aplicación de la política incluye las siguientes fases:

- Determinación del alcance: determinar las fuentes de información y la ciberinformación que se compartirá por medio de la política;
- Selección de las herramientas que se utilizarán para el intercambio de ciberinformación;
- Selección de un Punto de Contacto (POC) de la red de intercambio de ciberinformación y desarrollo de procesos para ir actualizando la información del POC;
- Prueba de sistemas y procesos para el intercambio de ciberinformación y ajustes necesarios;
- Lanzamiento del sistema de intercambio de ciberinformación (puesta en marcha);
- Monitoreo y control continuos
- Examen y mejoramiento continuos

3. GESTIÓN DE LA CIBERINFORMACIÓN Y SU INTERCAMBIO

3.1 Tipos de ciberinformación

Se puede compartir la siguiente ciberinformación.

CIBERINTELIGENCIA

- **Inteligencia de ciberamenazas (CTI)**: incluye un panorama de las ciberamenazas, inteligencia sobre los deseos de los *hackers*, etc.
  - **CTI Estratégica:** la información estratégica ayuda a una organización a entender el tipo de ciberamenazas y las capacidades y motivaciones de quienes perpetran ataques.
    - Contribuye a formular una imagen general de la intención y las capacidades de las ciberamenazas maliciosas.
    - Informa la toma de decisiones y/o proporciona alertas tempranas.
    - Puede incluir tendencias (por ejemplo, objetivos, comportamientos de atacantes), estadísticas, información sobre ciberamenazas (por ejemplo, amenazas persistentes avanzadas (APT), informes de ciberincidentes, documentos de política, documentos técnicos o de investigación), etc.
    - *Un ejemplo de CTI estratégica es un informe amplio sobre las nuevas ciberamenazas a la infraestructura crítica de un Estado, en el que se describen posibles vulnerabilidades y vectores de ataque. Este informe suele ser utilizado por quienes tienen la responsabilidad de tomar decisiones de alto nivel para formular políticas y estrategias de ciberseguridad de largo plazo.*
  - **CTI Operacional:**
    - Proporciona contexto acerca de los ciberincidentes, y de ese modo contribuye a que quienes están a cargo de la protección detecten cualquier posible peligro.
    - Permite determinar los impactos que podrían tener los ciberincidentes en las operaciones (por ejemplo, tácticas, técnicas y procedimientos (TTP), motivos, impacto, momento).
    - Ayuda a asignar recursos y priorizar tareas.
    - *Un ejemplo de CTI operacional es la información sobre una campaña de* phishing *que se esté desarrollando y tenga como blanco de ataque a la aviación. Esto incluye detalles como las técnicas, tácticas y los procedimientos que utilizan los actores de amenazas. Esta información es valiosa para que los equipos de operaciones de seguridad detecten y respondan a ciberamenazas inmediatas.*
  - **CTI táctica:** inteligencia utilizada por las organizaciones para ayudar a desarrollar proactivamente una postura de seguridad que pueda resistir ataques (por ejemplo, Indicadores de Compromiso (IoC), TTP, vulnerabilidades).
    - *Un ejemplo de CTI táctica son los indicadores de compromiso relacionados con una variante específica de un programa informático malicioso (*malware*). Esto incluye direcciones IP específicas, etiquetas (*hash*) de archivos y patrones de comportamiento asociados con el programa malicioso. Esta información táctica es utilizada por analistas de ciberseguridad de primera línea para identificar y mitigar ciberamenazas en tiempo real.*

- **Indicadores de Compromiso (IoC)**: Las IoC son, por ejemplo, direcciones IP maliciosas, URL maliciosas, nombres de dominio maliciosos o *malware hash*.
  - Compartir esta información ayudará a las partes destinatarias a proteger mejor sus sistemas/servicios.
  - Al compartir los IOC, no hay necesidad de revelar quién los descubrió.

- **Tácticas, técnicas y procedimientos (TTP):** Los TTP son escenarios de ataques y métodos preferidos por los *hackers*[7].

- **Vulnerabilidades:**
  - **Para la persona usuaria de un ciberactivo:** la ciberinformación que se compartirá está relacionada principalmente con el ciberactivo (por ejemplo, equipos, programas informáticos, servicio, protocolo, estándar) respecto del cual se detectó la vulnerabilidad. No sería útil compartir información relativa a la identidad de la persona usuaria del ciberactivo.
    - La información puede compartirse con otras personas para ayudarlas a protegerse.
    - No es necesario revelar quién descubrió la vulnerabilidad.
    - Con respecto a la divulgación responsable de vulnerabilidades, el programa de gestión de vulnerabilidades de la organización puede proponer un "cuadro de honor" o un proceso similar para expresar el reconocimiento a quienes investigan por su contribución a la detección de vulnerabilidades.
  - **Para la persona propietaria de un ciberactivo:** la persona propietaria del ciberactivo debería compartir la información sobre las vulnerabilidades que afectan a dicho activo con quienes lo utilizan.
    - La persona o entidad propietaria del ciberactivo también debe proponer un parche / arreglo.
    - Las mejores prácticas incluyen compartir información sobre esas vulnerabilidades con los CERT/CSIRT (nacionales o sectoriales) para ayudarles a responder ante cualquier ciberincidente relacionado con el ciberactivo pertinente.
  - Se puede considerar una diferencia entre vulnerabilidades potenciales, confirmadas y explotadas en cuando a cómo tratar el intercambio de información relacionada con esas vulnerabilidades.

INFORME SOBRE CIBERINCIDENTES

- Contiene información sobre un ciberincidente que afecta a una organización.
- En lo posible, en los informes de ciberincidentes, se debería incluir la siguiente información: resumen, tipo, fecha y hora exactas del incidente, ubicación, duración, cronología (es decir, secuencia de eventos), IoC, TTP, contexto, vulnerabilidad(es), impactos (seguridad operacional, seguridad de la aviación, eficiencia, capacidad, actividad, finanzas, reputación), gravedad, motivación, contra quién va dirigido, actor de la amenaza, servicios y organización u organizaciones afectadas, etc.
- Por regla general, cuanta más información se proporcione en el informe, más se podrá actuar en consecuencia.

[7] MITRE ATT&CK ha desarrollado y mantiene una taxonomía de TTP que se puede encontrar en su sitio web: https://attack.mitre.org/

CIBERMITIGACIONES

- Contiene información sobre métodos para:
  - subsanar las vulnerabilidades;
  - mitigar ciberamenazas; y
  - responder ante ciberincidentes y recuperarse tras ellos.
- La información puede incluir parches para corregir vulnerabilidades, actualizaciones de antivirus para detener *exploits* (explotación de vulnerabilidades) e instrucciones para eliminar a los actores maliciosos de las redes.

CONCIENCIA DE LA SITUACIÓN

- Contiene información que proporciona a quienes toman decisiones telemetría en tiempo real de las vulnerabilidades explotadas, las amenazas activas y los ciberataques que puede ser necesaria para responder a un ciberincidente.
- También podría contener información sobre los blancos de ataques y el estado de las redes informáticas críticas, tanto públicas como privadas.

MEJORES PRÁCTICAS

- Contiene información relacionada con el desarrollo de programas informáticos y la prestación de servicios, como controles de seguridad, prácticas de desarrollo y respuesta a incidentes y parches de programas informáticos o mediciones de eficacia.

3.2 Emisores, destinatarios y fuentes de ciberinformación

- Para compartir ciberinformación, se requiere un emisor, un destinatario y una fuente de información (si la información no proviene del emisor).
- La siguiente tabla incluye ejemplos de emisores, destinatarios y fuentes de ciberinformación en la aviación civil.

Emisores/destinatarios	• Usuarios del espacio aéreo [por ejemplo: aerolíneas, aviación general, explotadores de sistemas de aeronaves no tripuladas (UAS)] • Proveedores de servicios de navegación aérea (ANSP) • Explotadores de aeropuerto • Autoridades [por ejemplo, la administración de aviación civil (CAA)] • Proveedores de servicios de aviación • Fabricantes • Cadena de suministro de la aviación y ajena a la aviación • Otros

Fuentes	• Emisores/destinatarios enumerados anteriormente • Aeronaves (por ejemplo, UAS, aviones) • Inteligencia de fuentes abiertas (OSINT) • Proveedores de CTI • Asociaciones y organizaciones internacionales (por ejemplo, asociaciones de aerolíneas/aeropuertos/ANSP) • Centros de ciberseguridad de la aviación internacional/nacional/regional y CERT/ISAC de aviación • Otros

- El apéndice A incluye el flujo recomendado de los diferentes tipos de ciberinformación que pueden intercambiarse entre las partes interesadas de la aviación.

3.3 Evaluación, análisis y etiquetado TLP de la ciberinformación que se compartirá como emisor

3.3.1 Evaluación y análisis

Antes de compartir ciberinformación, el emisor debería realizar un análisis con el fin de:

- evaluar la confiabilidad y fiabilidad de la fuente (véanse 3.3.1.1 y los apéndices B y D);
- analizar la verosimilitud/credibilidad de la información (véanse 3.3.1.2 y los apéndices C y D), y
- analizar la pertinencia de la información para su organización, la comunidad de intercambio de información [organización u organizaciones destinataria(s)] y el ecosistema de la aviación.

Este es un paso clave en el intercambio de ciberinformación. Sin este paso, la información se convierte en una colección de datos / hallazgos sin contexto.

Al realizar el análisis anterior, es importante recordar que:

- diferentes problemas analíticos requieren enfoques diferentes; y
- quienes los analizan deberían ser conscientes de sus sesgos naturales, y esforzarse al máximo por superarlos para realizar un análisis objetivo utilizando métodos y herramientas adecuados.

Para ilustrar el papel de la evaluación y el análisis de la ciberinformación, las figuras 2 y 3 que se encuentran a continuación describen la diferencia entre la información de fuentes abiertas y la inteligencia de fuentes abiertas, donde se hace evidente que la usabilidad de la información aumenta significativamente cuando se hace un análisis y aseguramiento adecuados antes de su difusión.

- **OSINF (Información de fuentes abiertas):** se trata de la información que se comparte tal cual fue recopilada.

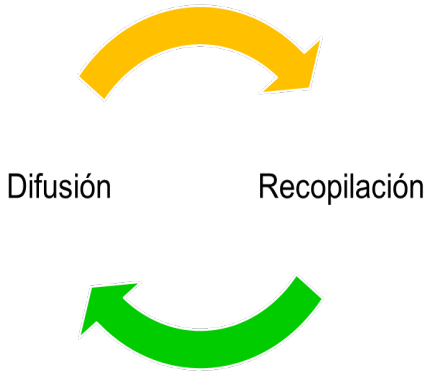

Figura 2. Información de fuentes abiertas

- **OSINT (Inteligencia de fuentes abiertas):** se trata de la información que se somete al proceso siguiente después de su recopilación.

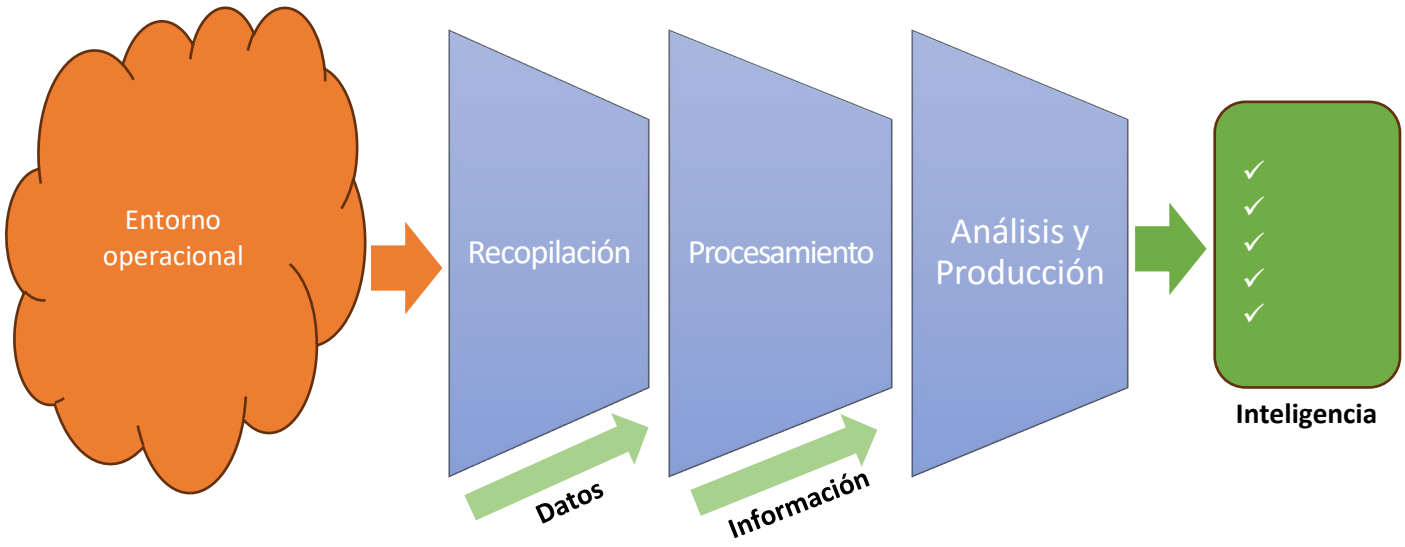

Figura 3. Producción de ciberinteligencia[8]

3.3.1.1 Evaluación de la fiabilidad y confiabilidad de la fuente

Evaluar el nivel de confiabilidad y fiabilidad de la fuente de ciberinformación/ciberinteligencia es crucial para tomar decisiones informadas.

El apéndice B incluye un ejemplo de marco para definir criterios y propone un sistema de evaluación para medir la fiabilidad y confiabilidad de una fuente de ciberinformación/ciberinteligencia.

Las ponderaciones y la escala de puntuación utilizadas en el apéndice B pueden ajustarse para ajustarse a los requisitos específicos de la organización y a su tolerancia al riesgo.

En el apéndice D figura otro ejemplo de sistema de confianza de la información para evaluar tanto la fiabilidad de la fuente como la credibilidad de la información (véase 3.3.1.2) utilizando un método diferente: el Código del Almirantazgo o Sistema de Clasificación de Inteligencia (el sistema de la OTAN).

Las organizaciones deberían reevaluar y actualizar periódicamente las puntuaciones de confianza a medida que el panorama de ciberamenazas y las fuentes de inteligencia de amenazas vayan evolucionando con el tiempo.

3.3.1.2 Análisis de la verosimilitud/credibilidad de la ciberinformación

Es esencial evaluar el nivel de verosimilitud/credibilidad de la ciberinformación/ciberinteligencia.

El apéndice C incluye un ejemplo de marco para definir criterios y propone un sistema de evaluación para medir la verosimilitud/credibilidad de la ciberinformación/ciberinteligencia.

Las ponderaciones y la escala de puntuación utilizadas en el apéndice C pueden adaptarse para que se ajusten a los requisitos específicos de la organización y a su tolerancia al riesgo.

[8] Adaptado de Joint Publication 2-0, *Joint Intelligence* (2013).

Las organizaciones deberían reevaluar y actualizar periódicamente las puntuaciones de verosimilitud/credibilidad a medida que se disponga de nueva información/inteligencia sobre ciberamenazas y el panorama de ciberamenazas vaya evolucionando.

En el apéndice D figura otro ejemplo de sistema de confianza de la información para evaluar tanto la fiabilidad de la fuente (véase 3.3.1.1) como la credibilidad de la información utilizando un método diferente: el Código del Almirantazgo o Sistema de Clasificación de Inteligencia (el sistema de la OTAN).

3.3.2 Sistema de etiquetas del Protocolo de Luces de Semáforo (TLP)[9,10]:

3.3.2.1 Utilización del TLP en la aviación

El estándar TLP comprende cinco etiquetas: RED, AMBER, AMBER+STRICT, GREEN y CLEAR.

Dado que la etiqueta **TLP:CLEAR** no restringe la difusión de la información recibida a nadie a través de ningún medio, y dado que la etiqueta **TLP:RED** limita la divulgación de la información a la(s) persona(s) destinataria(s) indicadas específicamente sin que sea posible ninguna divulgación ulterior, estas dos etiquetas no se examinan en esta sección. Las tres etiquetas que requerirían de algunas aclaraciones sobre cómo aplicarlas en un contexto de aviación son:

- **TLP:GREEN**
- **TLP:AMBER**
- **TLP:AMBER+STRICT**

TLP:GREEN	- La información marcada como TLP:GREEN se puede compartir dentro de la comunidad de la aviación. - La persona destinataria de la información TLP:GREEN puede a su vez distribuirla a cualquier organización de aviación (CAA, ANSP, explotadores de aeropuertos, usuarios del espacio aéreo, fabricantes, proveedores de servicios de aviación, etc.). - Esa información también se puede compartir con organizaciones de ciberseguridad que cumplan una función en la aviación (centros nacionales de ciberseguridad, CERT/CSIRT de aviación nacionales/regionales/internacionales, ISAC de aviación, etc.). - También puede compartirse con organizaciones ajenas a la aviación que utilicen tecnologías similares (por ejemplo, información relacionada con las tecnologías operacionales o de la información), compartan ciberamenazas similares o presten servicios a la aviación (por ejemplo, sistemas o servicios de telecomunicaciones, sistemas o servicios energéticos). Esas organizaciones ajenas a la aviación

[9] El Protocolo de Luces de Semáforo (TLP) es un estándar desarrollado por FIRST [Forum of Incident Response and Security Teams (Foro de equipos de seguridad y respuesta a incidentes)] para facilitar el intercambio de información con el público apropiado. Este documento proporciona orientación sobre el uso de la versión 2.0 del protocolo TLP, que puede consultarse en este enlace: https://www.first.org/tlp/.

[10] La guía de este documento reemplaza la “Orientación sobre el Protocolo del Semáforo” publicada por la OACI en 2021.

	pueden ser agentes de otros sectores (por ejemplo, explotadores, autoridades, fabricantes) u organizaciones relacionadas con la ciberseguridad (centros nacionales de ciberseguridad, CERT/CSIRT relacionados con otros sectores, ISAC de otros sectores).

TLP:AMBER	- La información marcada como TLP:AMBER puede ser compartida por la persona destinataria dentro de su organización y con sus clientes en función de **la necesidad de conocer** dicha información. - Aunque el significado de «organización» es simple, en la aviación el significado de "clientes" que tengan la **necesidad de conocer** debería interpretarse de la siguiente manera: o Las CAA pueden compartir este tipo de información: ▪ dentro de su Estado con: • partes interesadas de la aviación nacionales; • centro(s) nacional(es) de ciberseguridad; y • CERT/CSIRT(s) e ISAC(s) nacionales de aviación. ▪ fuera de su Estado, con: • otras CAA; y • CERT/CSIRT e ISAC nacionales/regionales/internacionales de aviación. o Las partes interesadas de la aviación (ANSP, explotadores de aeropuertos, usuarios del espacio aéreo, proveedores de servicios de aviación) pueden compartir este tipo de información con: ▪ sus CAA nacionales; ▪ organizaciones que contribuyan a su prestación de servicios; ▪ CERT/CSIRT e ISAC nacionales/regionales/internacionales de aviación; y ▪ sus clientes, excluidos los pasajeros y pasajeras (por ejemplo, agentes de viajes, puntos de venta libres de impuestos). o Los fabricantes pueden compartir este tipo de información con: ▪ CAA nacionales; ▪ sus clientes (por ejemplo, líneas aéreas, aeropuertos); ▪ CERT/CSIRT e ISAC nacionales/regionales/internacionales de aviación; y ▪ sus subcontratistas.
TLP:AMBER+STRICT	- La información marcada como TLP:AMBER + STRICT puede ser compartida por la persona destinataria solo dentro de su organización solo con quienes tengan **la necesidad de conocer** dicha información.

3.3.2.2 Etiquetas TLP recomendadas para distintos tipos de ciberinformación

Se recomienda seguir las siguientes pautas al etiquetar ciberinformación para su uso en la aviación. En algunos casos, como los que se indican a continuación, sin que la lista sea exhaustiva, es posible que, tras determinadas consideraciones, no se sigan las recomendaciones que figuran más abajo; por ejemplo:

- El etiquetado TLP podría evolucionar con el tiempo: la ciberinformación puede etiquetarse como más restrictiva cuando se comparte por primera vez, y luego, con el tiempo, se puede utilizar una etiqueta menos estricta si el riesgo de divulgar esa información disminuye.
- Perspectivas del Estado frente a la industria respecto del etiquetado: un Estado puede tener reglas diferentes para etiquetar la ciberinformación que una parte interesada de la aviación debido a diferentes consideraciones (por ejemplo, restricciones de seguridad nacional).
- Limitaciones nacionales aplicables a la industria: un Estado puede utilizar una etiqueta específica para determinado tipo de información que se aplique a las infraestructuras críticas nacionales (por ejemplo, divulgación inicial de IOC, como direcciones IP sospechosas).

CIBERINTELIGENCIA

- **Inteligencia de ciberamenazas (CTI):**
  - **CTI estratégica:** depende de las características de la CTI estratégica y del público (por ejemplo, junta directiva, nivel C, analista de CTI, equipo azul)
    - **TLP:RED**: inteligencia específica y muy sensible acerca de una ciberamenaza dirigida contra la organización. Solo necesita estar al tanto un número limitado de personas con autoridad para tomar decisiones.
    - **TLP:AMBER**: La administración superior, la junta directiva o quienes integran el comité de toma de decisiones deben estar al tanto de una ciberamenaza específicamente dirigida contra la organización, pertinente para la aviación (por ejemplo, la cadena de suministro, las partes interesadas conectadas) y/o relevante para la infraestructura crítica nacional.
    - **TLP:GREEN**: inteligencia que debe compartirse con una comunidad para que se conozca ampliamente y se actúe en consecuencia (por ejemplo, documentos de políticas, informes técnicos, tendencias, estadísticas).
  - **CTI Operacional:**
    - **TLP:RED**: para determinado personal operativo, técnico y de seguridad específico que necesite actuar en función de inteligencia específica respecto de una ciberamenaza concreta o un ciberincidente contra una parte interesada de la aviación pertinente o una infraestructura nacional esencial (por ejemplo, cadena de suministro, parte interesada conectada).
    - **TLP:AMBER**: para el personal operativo, técnico y de seguridad que necesite estar al tanto de una ciberamenaza o ciberincidente concretos dirigidos contra la organización o relacionado con la aviación o la infraestructura crítica nacional .
    - **TLP:GREEN**: inteligencia que debe compartirse con una comunidad para que se conozca ampliamente y se actúe en consecuencia.

- **CTI Táctica:**
  - **TLP:RED**: para determinado personal técnico y de seguridad que necesite actuar ante una ciberamenaza específica contra la organización o necesite estar al tanto de un ciberincidente en curso.
  - **TLP:AMBER**: para el personal técnico y de seguridad que necesite estar al tanto de una vulnerabilidad, o de una ciberamenaza o ciberincidente en curso dirigidos contra la organización o relacionados con la aviación o la infraestructura crítica nacional.
  - **TLP:GREEN**: inteligencia que debe compartirse con una comunidad para que se conozca ampliamente y se actúe en consecuencia.

- **IOCs**: **TLP:GREEN**

- **TTPs**: **TLP:GREEN**

- **Vulnerabilidades:**
  - Vulnerabilidad explotada: **TLP:RED**
  - Vulnerabilidad confirmada (con o sin parche): **TLP:AMBER**
  - Vulnerabilidad potencial sin parche: **TLP:AMBER**
  - Vulnerabilidad potencial sin parche: **TLP:GREEN**

INFORME SOBRE CIBERINCIDENTES

- Ninguna recomendación, ya que depende de la naturaleza, el contexto y el momento del incidente (es decir, el tiempo transcurrido entre el ciberincidente y el intercambio de información). **TLP:CLEAR** puede excluirse en las primeras etapas, pero, después de cierto tiempo, puede volverse aplicable.

3.4 Evaluación y análisis de la información por parte de quien la recibe

La persona destinataria debería analizar la ciberinformación recibida para asegurarse de que reúna las siguientes características:

1. **Confiable/segura/de buena calidad:** el nivel de confianza[11] en la ciberinformación quizás no sea suficiente para considerar que, como consecuencia de la recepción de la información, se deban tomar ciertas medidas.
2. **Pertinente:** un ejemplo de pertinencia es el siguiente: si la persona destinataria no puede actuar en función de la información (por ejemplo, no tiene necesidad de conocerla) mientras que esa misma información puede ser pertinente para otro personal de la organización. Esto puede ser un obstáculo si la información recibida es **TLP:RED**. En ese caso, quien reciba la información debería ponerse en contacto con quien la envía y pedir su consentimiento para reenviarla a la(s) persona(s) destinatarias interesadas mediante la recepción de una versión de la información con una etiqueta más baja, o para proporcionar a la persona emisora otra persona de contacto en la organización que pueda recibir la versión **TLP: RED** de la información.

[11] Véanse 3.3.1.1, 3.3.1.2 y los apéndices B, C y D.

3. **Que pueda dar lugar a una acción ejecutable:** la etiqueta TLP puede ser un impedimento para que la persona destinataria actúe en función de la información recibida, en cuyo caso se requeriría un debate adicional entre la persona emisora y la destinataria para permitir que se actúe en función de la información recibida. Por ejemplo:
    - Si la información está marcada con la etiqueta **TLP:RED** y la persona destinataria necesita coordinar con otras personas de la organización para actuar en consecuencia, pero esas otras personas no han recibido la misma información.
    - Si la información es **TLP:AMBER+STRICT** y la persona destinataria necesita interactuar con otra organización para actuar de acuerdo con el contenido que se comparte.

El análisis debería incluir además las siguientes actividades:

- La parte destinataria debería combinar la ciberinformación recibida con la inteligencia disponible (por ejemplo, correlacionarla y/o complementarla con otra información). Esto ayudará a aumentar o disminuir el nivel de confianza en esa información.
- La persona destinataria debería contextualizar la información en relación con sus funciones, lo cual resolvería cuestiones relacionadas con el significado de la información para quien la recibe en un contexto político, estratégico, operacional, técnico y/o de ciberseguridad.

3.5 Relación de confianza entre las partes

La confianza es un concepto dinámico y polifacético esencial para el intercambio seguro de información sensible. No es una medida absoluta sino relativa, que varía según el contexto, las relaciones y las conductas.

Establecer relaciones de confianza entre quienes emiten y quienes reciben la información es crucial para el intercambio efectivo de ciberinformación.

También puede ser necesario que haya una relación de confianza con socios o partes interesadas no tradicionales. Es importante identificar a las partes clave para el intercambio proactivo y/o reactivo de ciberinformación para que haya una difusión oportuna y pertinente.

Puede existir una relación de confianza con una variedad de socios y partes interesadas. Ejemplos de relaciones de confianza incluyen:

- Dentro de la aviación:
    - Entre organismos estatales (nacionales y/o internacionales)
    - De organismos estatales a organizaciones de aviación y viceversa
    - Entre organizaciones del sector
    - De organismos estatales u organizaciones de aviación a organizaciones internacionales (por ejemplo, OACI) y viceversa
- Con socios y partes interesadas no relacionados con la aviación:
    - Organizaciones no gubernamentales
    - Organizaciones sin fines de lucro
    - Organizaciones internacionales (por ejemplo, organismos pertinentes de las Naciones Unidas)
    - Organización Internacional de Policía Criminal (OIPC-INTERPOL)

Construir una relación de confianza normalmente lleva tiempo. Los Estados y las partes interesadas pueden establecer, cultivar y fomentar relaciones de confianza mediante:

- Alianzas con socios afines.
- Actividades regulares: participación en reuniones o conferencias periódicas.

- Acuerdos: las dos secciones siguientes proporcionan orientación sobre los tipos de acuerdos que se pueden concertar para el intercambio de ciberinformación.

Los Estados y las partes interesadas también deberían considerar los beneficios (véase la sección 1.1) y los costos asociados con establecer y cultivar relaciones de confianza, para justificar la inversión necesaria y tomar la decisión de hacerlo. Entre las cuestiones que deberían considerarse se incluyen:

- Tiempo: cuál es el compromiso de tiempo para establecer y desarrollar una relación.
- Recursos: incluidos los recursos humanos y financieros.
- Beneficios: qué recibe cada parte de la relación.
- Pasivos: pérdidas potenciales para cada parte por tener esa relación.
- Mantenimiento: también debe tenerse en cuenta el costo continuo de mantener una relación en términos de tiempo y recursos.

Mantener relaciones de confianza implica actividades como:

- Reuniones presenciales y virtuales: la frecuencia de las reuniones se acordará entre las partes. Se recomienda que se realicen según sea necesario, y al menos anualmente para reuniones presenciales, teniendo en cuenta el nivel de personal que participa (nivel superior, medio o técnico).
- Intercambio proactivo de ciberinformación: intercambio frecuente de información en función de necesidades y prioridades. Esta información puede incluir:
    - Cambios en las políticas y procedimientos que podrían afectar a las personas destinatarias.
    - Productos: informes puntuales, análisis estratégico, etc.
    - Información sin procesar: códigos fuente, registros, etc.
- Intercambio reactivo de ciberinformación: puede incluir compartir información relacionada con la respuesta a un ciberincidente:
    - Durante un ciberincidente: intercambio de información en tiempo real y en forma constante mientras el incidente está en curso.
    - Después de un ciberincidente: intercambio de hallazgos, análisis de la causa raíz, lecciones aprendidas, etc.

Las relaciones de confianza pueden terminarse si se pierde la confianza. Ejemplos de acciones que podrían conducir a ello son:

- Divulgación no autorizada de información clasificada: la divulgación accidental o deliberada de información clasificada a personas u organizaciones no autorizadas que puedan ser de seguridad nacional o contener información propietaria importante.
- Compartir deliberadamente información sensible: compartir intencionalmente información sensible de seguridad o información propietaria sensible con personas u organizaciones para exponer vulnerabilidades o dañar la credibilidad, especialmente si se difunde en el dominio público.

3.5.1 Acuerdos oficiales

El intercambio de ciberinformación entre las partes puede formalizarse mediante acuerdos bilaterales o multilaterales, vinculantes o no vinculantes.

Esos acuerdos incluyen diferentes tipos de partes. Por ejemplo, pueden concertarse acuerdos entre Estados, entre organismos estatales (por ejemplo, entre una administración de aviación civil y un organismo nacional de ciberseguridad del mismo Estado), entre organismos gubernamentales de diferentes Estados (por ejemplo, entre administraciones de aviación civil de diferentes Estados), entre un organismo estatal y partes interesadas de la aviación del mismo Estado, entre un organismo estatal y partes interesadas de la industria de otro Estado, o entre partes interesadas de la aviación.

En el apéndice E se proporciona una lista recomendada de las secciones que deberían incluirse en un acuerdo oficial de intercambio de ciberinformación para que las partes compartan funciones y responsabilidades claras, lo que, con el tiempo, se reflejará positivamente en el nivel de confianza entre las partes.

3.5.2 Acuerdos oficiosos

A menudo se recurre a acuerdos oficiosos cuando la confianza entre las partes que intercambian información ya está establecida o está implícita. Estos tipos de acuerdos deben utilizarse cuidadosamente, ya que no tienen consecuencias jurídicas para las partes signatarias. No deben ser el mecanismo principal ni único para el intercambio de ciberinformación.

Esos acuerdos incluyen información limitada que se necesita para que las partes compartan información, por ejemplo:

- los medios técnicos que se utilizarán para compartir información; y
- los puntos de contacto respectivos (datos individuales y del equipo).

Se debe poner énfasis en el uso riguroso y uniforme de las etiquetas del TLP cuando se comparte ciberinformación mediante acuerdos oficiosos para mantener y fomentar la confianza existente entre las partes.

4. ESTRUCTURACIÓN, COMUNICACIÓN Y ARCHIVO DE LA CIBERINFORMACIÓN COMPARTIDA

4.1 Estructuración de la ciberinformación para compartir

La ciberinformación debería estructurarse en función de taxonomías definidas o con una estructura definida de modo que se comparta con un contexto adecuado, así como con detalles útiles y que puedan traducirse en acciones concretas.

Este es un ejemplo de cómo estructurar la ciberinformación para ser compartida:

- Título: Descripción general de la ciberinformación
- Número de referencia: para que la persona emisora pueda rastrear la información
- Marcado con etiquetas TLP
- Principales aspectos, incluidos los siguientes, sin que la lista sea exhaustiva:
    - Categoría (por ejemplo, ciberespionaje, ciberdelitos, operaciones de información)
    - Tipo [por ejemplo: vulnerabilidad, *botnet* (red de bots), vigilancia, datos personales, redes sociales, filtración de credenciales, *phishing* (ciberestafas), ataques DDoS (ataques de denegación de servicios distribuidos), *malware (*programa maligno)]
    - Nivel de ciberamenaza (por ejemplo: crítico, alto, medio, bajo)
    - Dominio/sector
    - Confianza en la fuente de información y fiabilidad de la misma (véase 3.3.1.1)
- Puntos clave: lista de viñetas que explica la información
- Resumen
- Atribución: actor(es) de amenazas que podrían haber sido identificados potencial o realmente como perpetrador(es)
- Evaluación de impactos, objetivos, víctimas, etc.
- Recomendaciones sobre las medidas que debería(n) tomar la(s) persona(s) destinataria(s)
- Información que puede utilizarse para ejecutar una acción concreta
    - Ciberactivos afectados
    - Cronología
    - IoCs
    - Reglas de detección
    - TTP
- Mitigaciones
    - Mitigaciones genéricas
    - Mitigaciones específicas
- Referencias

4.2 Comunicación de ciberinformación

Esta sección proporciona orientación sobre las ventajas y desventajas de usar varios medios para compartir ciberinformación.

4.2.1 Por teléfono

Este tipo de comunicación es apta para la información marcada con la etiqueta TLP:RED, ya que permite una comunicación síncrona con la persona que recibe la información. También ayuda a comunicar información crítica que requiere una respuesta inmediata.

Si utiliza el teléfono para compartir ciberinformación, se recomienda el uso de controles para confirmar la identidad de ambas partes (por ejemplo, para evitar inyecciones de audio generadas por IA).

En general, este medio tiene una usabilidad limitada (se usa principalmente para compartir ciberinformación de alta urgencia y/o TLP:RED); por lo tanto, debería considerarse junto con otros medios de intercambio de ciberinformación.

4.2.2 Correo electrónico simple

La ciberinformación se puede compartir en texto plano en un correo electrónico.

Utilizar este medio para compartir ciberinformación implica que:

- La persona destinataria tiene que abrir el correo electrónico y leer la información.
- Es necesario que un(a) analista de CTI analice el contenido para evaluar si es pertinente para la persona destinataria.
- La información se procesará inicialmente en forma manual.

A continuación, se muestran algunas limitaciones del uso de mensajes de correo electrónico en texto plano para compartir ciberinformación:

- Este medio es apto para un contenido breve y en texto.
- Algunos sistemas de correo electrónico pueden bloquear el mensaje, ya que puede contener IOC, lo que activaría los controles de seguridad de IT.
- Es difícil mantener actualizadas las listas de correos electrónicos . Se recomienda el uso de direcciones de correo electrónico individuales y genéricas.
- La información marcada con etiqueta TLP:RED no se puede enviar a correos electrónicos genéricos (por ejemplo, groupmailbox@company.com), sino solo a correos electrónicos individuales (por ejemplo, alguien@company.com).
- Algunos tipos de direcciones de correo electrónico pueden no considerarse destinatarios de confianza (por ejemplo, direcciones de correo electrónico no profesionales alojadas en servicios comerciales de correo electrónico como gmail/hotmail/yahoo/etc.)
- Existe el riesgo de suplantación de correo electrónico. Por eso, se recomienda utilizar métodos de autenticación adecuados, como la firma digital de correo electrónico, para gestionar ese riesgo.

4.2.3 Correo electrónico con adjunto

La ciberinformación se puede compartir en un documento adjunto a un correo electrónico. El archivo adjunto se puede encriptar con una contraseña que se puede enviar a la persona destinataria a través de otro medio confiable (por ejemplo, mensajes de texto, aplicación de mensajería segura).

Utilizar este medio para compartir ciberinformación implica que:

- La persona destinataria tiene que abrir el correo electrónico y leer la información.
- Es necesario que un(a) analista de CTI analice el contenido para evaluar si es pertinente para la persona destinataria.
- La información se procesará inicialmente en forma manual.

A continuación, se enumeran algunas limitaciones del uso de mensajes de correo electrónico con adjuntos para compartir ciberinformación:

- Existe el riesgo de hacer clic en un archivo adjunto malicioso, por lo que el archivo adjunto debe desinfectarse primero.
- Algunos sistemas de correo electrónico bloquean algunos tipos de archivos adjuntos (por ejemplo, archivos comprimidos como archivos con extensiones .zip, .rar y .7z).
- Algunos sistemas de correo electrónico pueden bloquear el acceso al documento, ya que puede contener IOC, lo que activaría los controles de seguridad de IT.
- El tamaño del archivo adjunto puede impedir su transmisión por correo electrónico.
- Es difícil mantener actualizadas las listas de correos electrónicos . Se recomienda el uso de direcciones de correo electrónico individuales y genéricas.
- La información marcada con etiqueta **TLP:RED** no se puede enviar a correos electrónicos genéricos (por ejemplo, groupmailbox@company.com), sino solo a correos electrónicos individuales (por ejemplo, alguien@company.com).

4.2.4 Repositorio privado

La ciberinformación se puede compartir mediante el acceso a un repositorio privado que contiene la información que se compartirá.

En ese caso, deberían establecerse métodos para notificar a la(s) persona(s) destinataria(s) de que pueden acceder a nueva ciberinformación.

Esta notificación puede automatizarse de modo que se efectúe por correo electrónico u otros medios (por ejemplo, mensajes de texto, aplicación de comunicación segura).

El acceso al repositorio se debe proteger y mantener actualizado:

- Deberían aplicarse controles o protección de seguridad acordes con la sensibilidad de la información que se comparta en el repositorio. Los controles podrían incluir alojamiento de repositorios (por ejemplo, servidor privado/compartido, alojamiento en la nube), control de acceso/derechos, métodos de autenticación de usuarios [por ejemplo, inicio de sesión único (SSO), autenticación de dos/múltiples factores (2FA/MFA), etc.]
- La lista de organizaciones o personas autorizadas a acceder al archivo debería mantenerse continuamente actualizada para asegurarse de que esté al día y sea auténtica.
- Los derechos de acceso, lectura y escritura deberían proporcionarse a cuentas individuales y mantenerse actualizados.
- Deberían registrarse y analizarse todos los accesos y acciones que ocurran en el repositorio.
- La ciberinformación publicada en el repositorio debe catalogarse cuidadosamente en carpetas, ya que no todas las personas participantes tienen el mismo acceso a la información. Además, es necesario traspasar la información entre carpetas a medida que la clasificación (por ejemplo, etiqueta TLP) de la información vaya cambiando con el tiempo (por ejemplo, puede ser accesible a un público más amplio si se reduce la clasificación/etiquetado TLP). Esto puede convertirse en un proceso complejo a medida que vaya aumentando el número de miembros de la comunidad, así como la cantidad de información compartida en el repositorio.

4.2.5 Solicitudes

Se pueden utilizar varias aplicaciones de software (de código abierto o comerciales) para compartir ciberinformación (por ejemplo, MISP, OpenCTI, CyWare, etc.).

No es posible proporcionar una lista genérica de consideraciones para las aplicaciones en general, ya que esto depende de la naturaleza de la aplicación (por ejemplo, código abierto o comercial), quién se encarga de desarrollar y actualizar los controles de seguridad, los derechos de acceso, la catalogación de la información (por ejemplo, manual o automática, a través de reglas), el almacenamiento de información sensible (por ejemplo, servidores seguros / privados o públicos), etc. Por lo tanto, se recomienda evaluar todos esos aspectos, y otros según sea necesario, al considerar el uso de aplicaciones para el intercambio de ciberinformación.

Entre las aplicaciones existentes, en el apéndice F se proporciona información sobre *MISP - Open Source Threat Intelligence and Sharing Platform* (Plataforma de Código Abierto de Intercambio e Inteligencia de Amenazas), ya que la plataforma proporciona características interesantes que contribuirían a las iniciativas del sector de la aviación para compartir ciberinformación.

4.3 Archivo de la ciberinformación

Tanto el emisor como el destinatario deberían archivar la ciberinformación compartida para llevar un registro y control de calidad.

Al archivar la información se deberían considerar los siguientes aspectos:

- Reglamentación: debería tenerse en cuenta toda reglamentación que pueda aplicarse al archivo de información (por ejemplo, las leyes de privacidad y sus requisitos para archivar tipos específicos de información y la duración máxima permitida para mantener esa información en archivos).
- Medios de almacenamiento: el uso de medios de almacenamiento depende del tipo de información. Se pueden utilizar diferentes tipos de medios para archivar ciberinformación. Por ejemplo, los informes de ciberincidentes se pueden almacenar en una base de datos independiente específica; los informes de inteligencia de ciberamenazas, como archivo en un disco de computadora, etc.
- Control de acceso y derechos: el acceso a la ciberinformación archivada debe determinarse en una política que defina quién puede acceder a qué tipo de información. Esto va en línea con el marcado de la información con etiquetas TLP (por ejemplo, **TLP:AMBER+STRICT** no significa que la información pueda compartirse con todas las personas de la organización sino solo con las que necesitan conocerla).
- Accesibilidad local o a distancia: es posible que no se permita acceder a parte de la ciberinformación desde fuera de la organización (a través de intranets, por ejemplo), sino solo internamente. También es necesario otorgar derechos de acceso según las funciones y responsabilidades del personal que pueden utilizarse con fines de auditoría/aseguramiento.
- Protección/controles de seguridad: deberían aplicarse diferentes niveles de protección y controles de seguridad según el tipo de información. Por ejemplo, deberían implementarse controles más estrictos para proteger los informes de ciberincidentes que para proteger vulnerabilidades ya parcheadas.
- Relevancia: es posible que la evolución de los acontecimientos haga que la ciberinformación se vuelva obsoleta. Por ejemplo, las vulnerabilidades de sistemas que la organización ya no utiliza, inteligencia estratégica de ciberamenazas relacionadas con eventos geopolíticos que ya no existen, etc.

- Usabilidad: deben definirse diversas categorías de archivos para apoyar la continua usabilidad de la información. Por ejemplo:
    - “Caliente”: incluye datos recientes que se almacenan sin compresión en los archivos, lo que permite recuperarlos y procesarlos con el máximo rendimiento;
    - “Tibio”: incluye datos que se almacenan con una ligera compresión, lo que permite recuperarlos y procesarlos con muy buen rendimiento; y
    - “Frío”: incluye datos que han sido archivados y totalmente comprimidos, y que requieren de una recuperación y descompresión manual.
- Duración: el tiempo durante el cual se mantiene archivada la ciberinformación debería depender del tipo de información. Por ejemplo, se pueden definir reglas de archivo para que los IOC no tengan más de [X] años. Además, las acciones relacionadas con la eliminación de información obsoleta deberían llevarse a cabo como parte de los procesos para gestionar el archivo de ciberinformación.

5. POLÍTICA PARA EL REENVÍO DE CIBERINFORMACIÓN COMPARTIDA

5.1 Por qué reenviar ciberinformación compartida

Puede ser necesario reenviar a terceros la ciberinformación recibida de una fuente externa para dar a conocer esa información a un público más amplio que necesite estar enterado. Sin embargo, se debe considerar cuidadosamente si es apropiado compartir cualquier ciberinformación recibida.

A modo de ejemplo, un organismo estatal que recibe información de un originador que solo permite compartir esa información con entidades con las que tiene un acuerdo oficial. No obstante, el organismo estatal considera que otros organismos estatales que no tienen un acuerdo oficial con el originador de la información necesitan conocerla. En ese caso, quien haya recibido la información debería ponerse en contacto con el originador y solicitar su consentimiento para reenviarla a los demás organismos que necesiten conocerla.

Para determinar si la ciberinformación recibida se va a reenviar o no y a quién, quien la reciba debe considerar factores tales como los siguientes:

- Limitaciones del reenvío de información: ¿puede o debe compartirse esta información? En caso de duda (por ejemplo, duda de un posible uso indebido de la etiqueta TLP), la persona destinataria puede solicitar autorización a la persona emisora para compartir a su vez esa información con alguien más.
- El propósito del reenvío de la información recibida y la función de la persona a la que se está considerando como posible destinataria.

El propósito de compartir con otra persona la ciberinformación recibida depende de qué acciones se espera que ejecute la persona destinataria:

- Para información/concientización: la persona a la que se prevé reenviar la información necesita tener conocimiento de ella, y la información se comparte solo con fines informativos.
- Para actuar: la persona a la que se prevé reenviar la información necesita tener conocimiento de ella, y la ciberinformación se comparte además para que la persona destinataria realice una acción específica. Esa acción puede incluir:
  - Asignar o movilizar recursos para resolver un problema en particular.
  - Asignar o movilizar recursos para mitigar una ciberamenaza o vulnerabilidad en particular.
  - Asignar o movilizar recursos para asistir en la respuesta.

La función de la persona a la que se prevé reenviar información puede ser un factor que incida en la decisión de reenviar o no la ciberinformación. Algunas de las funciones para las que puede ser necesario tener conocimiento de la información son las que desempeñan:

- **Especialistas técnicos(as)**: personas expertas o especialistas que se encargan de supervisar la protección de redes, sistemas, servicios, aplicaciones, infraestructuras IT/OT, etc., de cualquier acceso no autorizado.
- **Personas responsables de elaborar políticas**: las personas que redactan estrategias, políticas, procedimientos y/o procesos de ciberseguridad relacionados o no con la aviación que deben poner en práctica las partes interesadas de la aviación.
- **Personas responsables de la toma de decisiones:** miembros del personal de nivel superior que aprueba la aplicación de estrategias, políticas, procedimientos y/o procesos de ciberseguridad en el ámbito de la aviación o en otros pertinentes.
- **Personas coordinadoras:** especialistas en ciberseguridad con la función de canalizar eficazmente la información compartida al personal adecuado.

- **Especialistas en seguridad operacional**: especialistas en seguridad operacional aérea que pueden determinar cuál será el posible impacto en la seguridad operacional, eficiencia y/o capacidad de la aviación.
- **Especialistas en seguridad de la aviación**: especialistas en seguridad de la aviación que pueden determinar cuál será el posible impacto en la seguridad de la aviación.

5.2 Reglas para el reenvío de ciberinformación

Las reglas para el reenvío de ciberinformación incluyen muchos aspectos que deben considerarse cuidadosamente:

- La organización con la que se prevé compartir la información (por ejemplo, Estado/parte interesada de la aviación/parte interesada ajena a la aviación, entidad nacional/internacional).
- La función que ejerce la persona destinataria con la que se prevé compartir la ciberinformación.
- Qué se compartirá: la ciberinformación completa o un extracto (por ejemplo, todo el documento o solo los párrafos relevantes).
- En qué circunstancias se compartirá la información: de manera proactiva o reactiva.
- Frecuencia de reenvío: de rutina o según sea necesario.
- Por qué se comparte la ciberinformación (por ejemplo, para información o acción).
- Manejo de la ciberinformación: todas las clasificaciones y advertencias originales deben permanecer en los canales de comunicación apropiados (es decir, canales de comunicación clasificados y no clasificados).
- La etiqueta TLP no se puede cambiar al reenviar la ciberinformación.

5.3 Método y medios para el reenvío de información

El método/medio para el reenvío de ciberinformación debe ser seguro y simple, según corresponda.

Información física: Información que se proporciona en copia impresa. Se recomienda empaquetar adecuadamente la información (por ejemplo, en una carpeta) y asegurarla para que permanezca cerrada (por ejemplo, un folio que cierre con cremallera o pestillo) durante su traslado al lugar de la reunión y antes de proporcionar la(s) copia(s) impresa(s). Cualquier recordatorio o advertencia sobre el manejo de la información debería anotarse en la propia información o en una carátula (por ejemplo, las advertencias sobre el manejo de la información confidencial de seguridad (SSI)[12] generalmente se incluyen en una carátula con instrucciones).

Información electrónica: Los mismos medios para compartir ciberinformación descritos en la sección 4.2 se aplican al reenvío de ciberinformación. Sin embargo, se recomienda tener en cuenta que es posible que la persona con la que se prevé compartir la ciberinformación no tenga acceso al medio electrónico al que tiene acceso la persona emisora (por ejemplo, su dirección de correo electrónico puede no estar incluida en la lista de personas autorizadas a acceder al portal o repositorio donde está alojada la información).

Existen reglas adicionales para el manejo de la información clasificada que varían según el Estado o la organización. Esas reglas deben respetarse estrictamente de conformidad con las normas y procedimientos aplicables.

— — — — — — — —

[12] En la Sección 2.3 del *Manual de Seguridad de la Aviación* de la OACI (Doc. 8973 – De distribución limitada), se proporciona información útil que puede aplicarse a un contexto de intercambio de ciberinformación.

Apéndice A
Ciberinformación que se recomienda compartir en la aviación según el tipo de información

CIBERINTELIGENCIA

- **Inteligencia de ciberamenazas (CTI):**
  - **CTI estratégica:**
    - De los organismos estatales (centro nacional de ciberseguridad, CAA, etc.) a las partes interesadas de la aviación del mismo Estado
    - Del centro nacional de ciberseguridad a los CERT/ISAC de aviación
    - De los CERT/ISAC de aviación a las partes interesadas de la aviación
    - Entre los centros nacionales de ciberseguridad de confianza
    - Entre Estados de confianza
  - **CTI Operacional:**
    - Entre partes interesadas de la aviación
    - De los CERT/ISAC de aviación a las partes interesadas de la aviación
    - De partes interesadas de aviación a organismos del mismo Estado (centro nacional de ciberseguridad, CAA, etc.)
  - **CTI Táctica:**
    - Entre partes interesadas de la aviación
    - De los CERT/ISAC de aviación a las partes interesadas de la aviación
    - Del centro nacional de ciberseguridad a los CERT/ISAC de aviación
    - Del centro nacional de ciberseguridad a las partes interesadas de la aviación del mismo Estado
    - De partes interesadas de aviación a organismos del Estado (centro nacional de ciberseguridad, CAA, etc.)

- **IOCs**:
  - Entre partes interesadas de la aviación
  - De los CERT/ISAC de aviación a las partes interesadas de la aviación
  - Del centro nacional de ciberseguridad a los CERT/ISAC de aviación
  - Del centro nacional de ciberseguridad a las partes interesadas de la aviación del mismo Estado
  - De las partes interesadas de la aviación al centro nacional de ciberseguridad del Estado

- **TTPs**:
  - Entre partes interesadas de la aviación
  - De los CERT/ISAC de aviación a las partes interesadas de la aviación
  - Del centro nacional de ciberseguridad a los CERT/ISAC de aviación
  - Del centro nacional de ciberseguridad a las partes interesadas de la aviación del mismo Estado
  - De las partes interesadas de la aviación al centro nacional de ciberseguridad del Estado

- **Vulnerabilidades:**
  - Entre partes interesadas de la aviación
  - De las partes interesadas de la aviación a sus proveedores de la cadena de suministro
  - De investigadores(as) a CERT/ISAC de la aviación
  - De investigadores(as) a organismos del Estado (centro nacional de ciberseguridad, CAA, etc.)
  - De investigadores(as) a partes interesadas de la aviación
  - De investigadores(as) a la cadena de suministro
  - De los CERT/ISAC de aviación a las partes interesadas de la aviación
  - Del centro nacional de ciberseguridad a los CERT/ISAC de aviación
  - Del centro nacional de ciberseguridad a las partes interesadas de la aviación del mismo Estado
  - De las partes interesadas de la aviación a organismos del Estado (centro nacional de ciberseguridad, CAA, etc.)

INFORME SOBRE CIBERINCIDENTES

- Informes obligatorios sobre ciberincidentes (mediante leyes y/o reglamentos nacionales aplicables):
  - De las partes interesadas de la aviación a organismos pertinentes del Estado (centro nacional de ciberseguridad, CAA, etc.) (para incidentes de seguridad operacional y/o de seguridad de la aviación)
  - De las partes interesadas de la aviación a las autoridades policiales (para incidentes específicos relacionados con ciberdelitos, como el fraude, o con leyes específicas como las leyes de privacidad)
  - Del Estado a la OACI (para ciberincidentes relacionados con actos de interferencia ilícita)

- Notificación voluntaria de ciberincidentes
  - De las partes interesadas de la aviación al centro nacional de ciberseguridad
  - Entre partes interesadas de la aviación (especialmente si están interactuando)
  - De partes interesadas de la aviación a CERT/ISAC de aviación

— — — — — — — —

Apéndice B
Ejemplo de marco para evaluar y clasificar la fiabilidad y confiabilidad de una fuente de ciberinformación/ciberinteligencia

1. Reputación y trayectoria:
   - Evalúe el historial y la reputación de la fuente en la comunidad de ciberseguridad.
   - Busque éxitos pasados, contribuciones y su participación en organizaciones de la industria.
   - Evalúe su historial al proporcionar información/inteligencia exacta y oportuna sobre ciberamenazas.

2. Credibilidad y experiencia:
   - Evalúe las calificaciones, certificaciones y experiencia de las personas o equipos que rodean a la fuente.
   - Considere su experiencia en el ámbito específico de la información / inteligencia sobre ciberamenazas.

9. Fuentes de datos y métodos de recopilación:
   - Examine las fuentes y los métodos de recopilación de datos de la fuente.
   - Determine si tiene acceso a fuentes de datos diversas y confiables.
   - Evalúe el rigor de sus procesos de recopilación de datos.

4. Intercambio de datos y colaboración:
   - Determine si la fuente comparte información/inteligencia sobre ciberamenazas con organizaciones de confianza o pares del sector.
   - La colaboración con otras entidades de ciberseguridad puede mejorar la credibilidad.

5. Transparencia:
   - Evalúe el nivel de transparencia de sus informes y metodologías.
   - Evalúe si la fuente divulga sus fuentes de datos, técnicas de análisis y frecuencia de actualización.

6. Puntualidad y exactitud:
   - Evalúe la capacidad de la fuente para proporcionar información/inteligencia oportuna y exacta sobre ciberamenazas.
   - Considere su desempeño histórico en la predicción y detección de ciberamenazas.

7. Análisis y contexto:
   - Evalúe la profundidad y calidad de su análisis de las ciberamenazas.
   - Evalúe su capacidad de proporcionar contexto sobre las ciberamenazas, incluida la atribución y los posibles impactos.

8. Alineación con las normas de la industria:
   - Determine si la fuente respeta las normas de la industria y las mejores prácticas relativas a la información / inteligencia sobre ciberamenazas; por ejemplo, la adhesión a marcos como STIX / TAXII y formatos de datos comunes.

9. Cumplimiento legal y ético:
   - Asegúrese de que la fuente cumpla con las normas legales y éticas relativas a la recopilación y el intercambio de datos.

Para medir el nivel de confiabilidad de una fuente de ciberinformación/ciberinteligencia, se puede utilizar un sistema de puntuación basado en los criterios enumerados.

A continuación, se presenta un ejemplo de plan de evaluación.

1. Asigne una ponderación a cada criterio en función de su importancia para las necesidades específicas y el perfil de riesgo de su organización.
2. Califique la fuente en una escala (por ejemplo, 1-5) para cada criterio, siendo 5 el nivel más alto de confianza.
3. Calcule el puntaje total de confianza sumando las puntuaciones ponderadas para cada criterio. Cuanto más alta la puntuación, más confiable es la fuente.

He aquí un ejemplo simplificado de cómo calcular el puntaje total de confianza:

- Reputación y trayectoria: 4/5
- Credibilidad y experiencia: 5/5
- Fuentes de datos y métodos de recopilación: 3/5
- Intercambio de datos y colaboración: 4/5
- Transparencia: 4/5
- Puntualidad y exactitud: 4/5
- Análisis y contexto: 5/5
- Alineación con las normas de la industria: 4/5
- Cumplimiento legal y ético: 5/5

El puntaje total de confianza de la fuente podría ser:

(4*0,1) + (5*0,15) + (3*0,1) + (4*0,1) + (4*0,1) + (4*0,1) + (5*0,15) + (4*0,1) + (5*0,1) = **4,30**

— — — — — — — —

Apéndice C
Ejemplo de marco para evaluar la verosimilitud/credibilidad de la ciberinformación/ciberinteligencia

1. Corroboración con múltiples fuentes:
- Evaluar si múltiples fuentes independientes corroboran la información/inteligencia sobre ciberamenazas; por ejemplo, si múltiples fuentes proporcionan la misma información, puede aumentar la verosimilitud.

2. Coherencia con las amenazas y tácticas conocidas:
- Determine si la información/inteligencia sobre ciberamenazas es acorde con ciberamenazas, técnicas de ataque y tácticas conocidas; por ejemplo, si lo informado no es acorde con lo habitual, esto puede indicar un nivel más bajo de verosimilitud.

9. Detalles técnicos y evidencia:
- Examine si hay detalles técnicos y pruebas que respalden la información / inteligencia sobre ciberamenazas; por ejemplo, si hay evidencia técnica sólida, aumenta la verosimilitud.

4. Atribución y motivación:
- Evalúe la atribución de la ciberamenaza a actores o grupos específicos.
- Analice la motivación de esos actores y si esa motivación se corresponde con la ciberamenaza reportada.

5. Momento y contexto:
- Analice el momento de la ciberamenaza y su contexto dentro del panorama de la ciberseguridad.
- Considere si la ciberamenaza es acorde con los eventos o tendencias actuales.

6. Historial de denuncias exactas:
- Evalúe si la fuente tiene un historial de denuncias de ciberamenazas que resultaron ser exactas; por ejemplo, si la fuente tiene un historial de denuncias exactas, su verosimilitud aumenta.

7. Validación por pares y grupos de confianza:
- Determine si la información/inteligencia sobre ciberamenazas ha sido validada o respaldada por pares o grupos de confianza del sector; por ejemplo, si hay pares que validen la información, la información puede ser más verosímil.

8. Señales de alerta y anomalías:
- Preste atención a señales de alerta, anomalías o elementos sospechosos en la información / inteligencia sobre ciberamenazas; abordar y explicar estos problemas puede mejorar la verosimilitud.

Para medir el nivel de verosimilitud y confiabilidad de la ciberinformación / ciberinteligencia, se puede utilizar un sistema de puntuación basado en los criterios enumerados.

A continuación, se muestra un ejemplo de sistema de puntuación.

1. Asigne una ponderación a cada criterio en función de su importancia para las necesidades específicas y el perfil de riesgo de su organización.
2. Califique la fuente en una escala (por ejemplo, 1-5) para cada criterio, siendo 5 el nivel más alto de verosimilitud.
3. Calcule el puntaje total de verosimilitud sumando las puntuaciones ponderadas para cada criterio. Una puntuación más alta indica un informe de inteligencia de amenazas más creíble.

He aquí un ejemplo simplificado de cómo calcular el puntaje total de verosimilitud/credibilidad:

- Corroboración con múltiples fuentes: 4/5
- Coherencia con las amenazas y tácticas conocidas: 3/5
- Detalles técnicos y evidencia: 5/5
- Atribución y motivación: 4/5
- Momento y contexto: 4/5
- Historial de denuncias exactas: 4/5
- Validación por pares y grupos de confianza: 4/5
- Señales de alerta y anomalías: 3/5

La puntuación global de verosimilitud/credibilidad podría ser:

(4*0,15) + (3*0,15) + (5*0,15) + (4*0,1) + (4*0,15) + (4*0,1) + (4*0,1) + (3*0,1) = **3,90**

— — — — — — — —

Apéndice D
Ejemplo de plan de confiabilidad de la ciberinformación

En este apéndice se describe el Código del Almirantazgo[13] como otro ejemplo de método para evaluar los elementos de inteligencia recopilados.

La escala se puede utilizar cuando se comparte información para estimar la fiabilidad de la fuente y la credibilidad de la información. El método consiste en una notación de dos caracteres (una letra y un número); la letra evalúa la fiabilidad de la fuente y el número refleja la valoración del nivel de fiabilidad de la información.

Fiabilidad de la fuente

La fiabilidad de una fuente se determina sobre la base de una evaluación técnica de su capacidad o, en el caso de las fuentes de inteligencia humana, de su historial. La notación utiliza codificación alfabética de la A a la F para puntuar la fiabilidad de la fuente de la siguiente manera.

Código de fiabilidad	Fiabilidad	Explicación
A	Completamente fiable	Sin duda de autenticidad, confiabilidad o competencia; tiene un historial de completa fiabilidad.
B	Usualmente fiable	Duda menor sobre autenticidad, confiabilidad o competencia; tiene un historial de información válida la mayor parte del tiempo.
C	Bastante fiable	Duda de autenticidad, confiabilidad o competencia, pero ha proporcionado información válida en el pasado.
D	Usualmente no fiable	Duda significativa respecto de autenticidad, confiabilidad o competencia, pero ha proporcionado información válida en el pasado.
1.7	No fiable	Falta de autenticidad, confiabilidad y competencia; historial de información no válida.
F	No se puede determinar la fiabilidad	No existe ninguna base para evaluar la fiabilidad de la fuente.

[13] Los detalles del método se pueden encontrar en las páginas 59 a 60 de la publicación *Joint Doctrine 2-00, Intelligence, Counter-intelligence and Security Support to Joint Operations* (Cuarta edición), disponible aquí: https://www.gov.uk/government/publications/jdp-2-00-understanding-and-intelligence-support-to-joint-operations

Credibilidad de la información

La credibilidad de la información se evalúa en función de la probabilidad y los niveles de corroboración con otras fuentes. La notación utiliza codificación numérica del 1 al 6 para puntuar la credibilidad de la fuente de la siguiente manera.

Puntaje de credibilidad	Credibilidad	Explicación
1	Confirmada por otras fuentes	Confirmada por otras fuentes independientes; lógica en sí misma; coherente con otras informaciones sobre el tema.
2	Probablemente cierta	No confirmada; lógica en sí misma; coherente con otras informaciones sobre el tema.
3	Posiblemente cierta	No confirmada; razonablemente lógica en sí misma; concuerda con otras informaciones sobre el tema.
4	Dudosa	No confirmada; posible pero no lógica; no hay ninguna otra información sobre el tema.
5	Improbable	No confirmada; no lógica en sí misma; se contradice con otras informaciones sobre el tema.
6	No se puede determinar si es verdadera	No hay elementos para evaluar la validez de la información.

Las tablas anteriores se pueden combinar en la siguiente tabla.

Fiabilidad de la fuente		Credibilidad de la ciberinformación	
A	Completamente fiable	1	Confirmada por otras fuentes
B	Usualmente fiable	2	Probablemente cierta
C	Bastante fiable	3	Posiblemente cierta
D	Usualmente no fiable	4	Dudosa
E	No fiable	5	Improbable
F	No se puede determinar la fiabilidad	6	No se puede determinar si es verdadera

Estos son dos ejemplos de calificaciones de la ciberinformación compartida:

- *C4 que se traduce en: fuente bastante fiable e información dudosa.*
- *A1 que se traduce en: fuente totalmente fiable e información confirmada por otras fuentes.*

Si bien la evaluación es subjetiva, la calificación proporciona una herramienta útil que ayuda a la persona destinataria de la ciberinformación a efectuar su propia evaluación y análisis de la ciberinformación.

— — — — — — — —

Apéndice E
Estructura recomendada de un acuerdo oficial de intercambio de ciberinformación

Un acuerdo oficial de intercambio de ciberinformación debería incluir las siguientes secciones:

- ✓ Un preámbulo que incluya los nombres y la descripción de las partes.
- ✓ Definiciones y acrónimos
- ✓ Alcance: describe el alcance del documento y remite al apéndice 1, que indica el tipo de ciberinformación que ha de compartirse.
- ✓ Derechos y obligaciones de la persona receptora de la información (persona destinataria).
- ✓ Fuentes de información: quién proporcionará qué información a quién y en base a qué fuentes, y si es necesario compartir la fuente de la información.
- ✓ Limitaciones sobre qué y con quién se puede compartir la información, teniendo en cuenta las leyes vigentes, los derechos de propiedad intelectual, la información comercial confidencial, la definición de etiquetas TLP, etc.
- ✓ Formato y frecuencia con que se intercambia información.
- ✓ Medios de transmisión de información (como cartas, teléfono, mensajes de texto, correo electrónico, repositorio, etc.), incluida la protección y el aseguramiento de la confidencialidad, integridad y disponibilidad de la información transmitida digitalmente.
- ✓ Requisitos de calidad: describe las acciones que debe realizar el emisor antes de transmitir información. También describe los medios para velar por la integridad y calidad de la información que se comparte, incluida, por ejemplo, su desidentificación y/o desinfección.
- ✓ Almacenamiento y mantenimiento de registros: describe políticas y procedimientos para archivar la información compartida. También describe el tiempo mínimo durante el cual la información enviada/recibida debe archivarse a efectos de control de calidad del acuerdo y la relación entre las partes.
- ✓ Costo: describe qué parte asume el costo de compartir información. Se recomienda que cada parte asuma sus propios gastos relacionados con la aplicación del acuerdo.
- ✓ Procedimientos de gobernanza y gestión de cambios en el acuerdo.
- ✓ Correspondencia y avisos relacionados con el acuerdo.
- ✓ Responsabilidad: donde se describen las responsabilidades respectivas. Se recomienda eximir a la parte emisora de la responsabilidad relacionada con la información compartida.
- ✓ Procesamiento de datos personales: describe cómo se van a tratar los datos personales, incluidas las leyes y reglamentos aplicables.
- ✓ Solución de controversias: cómo y en el marco de cuáles leyes se abordarán las controversias relacionadas con el acuerdo. Se recomienda que las partes traten de resolver las controversias de manera amistosa; y, de no llegarse a un acuerdo, por mediación en una jurisdicción acordada.
- ✓ Acuerdo completo y enmiendas: donde se describe la precedencia de las diversas partes del acuerdo.
- ✓ Fecha de entrada en vigor del acuerdo, duración y procedimientos para su renovación y terminación.
- ✓ Cesión: firmas de personas autorizadas para cada parte.
- ✓ Apéndices:
  - Apéndice 1 - Información que ha de proporcionarse: describe el tipo de información que compartirá cada una de las partes.
  - Apéndice 2: definición de etiquetas TLP, incluida la referencia a la norma FIRST TLP.

— — — — — — — —

Apéndice F
MISP - Plataforma de código abierto para inteligencia e intercambio de información sobre amenazas

MISP[14] es una plataforma para compartir, almacenar y correlacionar Indicadores de Compromiso (IoC) de ciberataques dirigidos, así como inteligencia de ciberamenazas, que puede incluir información sobre actores de amenazas, información de fraude financiero, etc.

Es una plataforma gratuita y de código abierto para el intercambio e inteligencia de ciberamenazas, que permite a las organizaciones crear comunidades para compartir información, como inteligencia de ciberamenazas, indicadores, información de actores de amenazas o cualquier tipo de ciberamenaza que se pueda estructurar en la MISP.

Los usuarios de MISP se benefician del conocimiento colaborativo sobre *malware* o ciberamenazas existentes. La MISP se utiliza mediante la creación de "comunidades". El intercambio de información ocurre dentro de una comunidad de usuarios. El objetivo de esta plataforma basada en la confianza es ayudar a mejorar las medidas para contrarrestar los ciberataques dirigidos, así como la ejecución de acciones preventivas y de detección.

Se recomienda que los Estados y las partes interesadas de la aviación consideren la MISP, así como cualquier plataforma equivalente, como medio o método para compartir ciberinformación, ya que la plataforma:

- contribuye a automatizar el uso de la información recibida para actualizar diversos sistemas de seguridad, como los centros de operaciones de seguridad y gestión de información y eventos (SIEM/SOC), cortafuegos, programas antivirus y sistemas de detección y prevención de intrusos/sistemas de prevención de intrusos (IDPS/IPS);
- permite compartir ciberinformación rápidamente, ya que el tiempo podría ser un factor crítico en caso de compartir información relacionada con una respuesta a un ciberincidente en curso;
- permite actualizar la ciberinformación relacionada con un ciberincidente con información adicional a medida que está disponible, y
- todos los tipos de información marcada con etiquetas TLP pueden compartirse a través de la MISP. Sin embargo, la información marcada como **TLP:RED** se comparte en la MISP solo cuando la comunidad está compuesta por un número limitado de personas que aceptan compartir dicha información. En general, la información **TLP:RED** no se comparte en la MISP sino a través de medios alternativos (por teléfono, mensajes de texto y por correo electrónico).

— FIN —

[14] Para más información sobre el uso del MISP: https://www.circl.lu/services/misp-malware-information-sharing-platform/