Propuesta integral para el fortalecimiento de la ciberresiliencia en los Centros de Comando y Control de la Fuerza Aeroespacial Colombiana

Mayor (FAC) Carlos Augusto Uribe Vergara

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (FAC) Carlos Augusto Uribe Vergara
Identificación	**:**	13743234
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Cr. Aldemar Serrano Cuervo
Tutor temático	**:**	PhD. Lina María Manrique Villanueva
Fecha de entrega	**:**	25 de agosto de 2025
Extensión	**:**	9564 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y que no esté disponible bajo una modalidad de acceso abierto.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Propuesta integral para el fortalecimiento de la ciberresiliencia en los Centros de Comando y Control de la Fuerza Aeroespacial Colombiana

Comprehensive proposal for strengthening cyber resilience in the Command and Control Centers of the Colombian Aerospace Force

Carlos Augusto Uribe Vergara[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este artículo examina la ciberresiliencia en los centros de comando y control de la Fuerza Aeroespacial Colombiana, con el objetivo de identificar fortalezas y áreas de mejora en su capacidad para enfrentar amenazas cibernéticas. El estudio emplea un enfoque mixto, basado en revisión documental, entrevistas a expertos y la aplicación de un modelo de ciberresiliencia y otro de evaluación de madurez, adaptado al contexto militar. Los resultados evidencian avances en la gestión de activos y controles, así como en la integración de mejores prácticas internacionales y nacionales. Sin embargo, se detectan brechas en la formalización de planes de continuidad y recuperación ante incidentes. Como conclusión, se proponen lineamientos estratégicos y técnicos enfocados en la gobernanza, la cultura organizacional, la arquitectura resiliente y la medición de la madurez, con el fin de fortalecer la sostenibilidad operativa y la protección digital en entornos críticos.

Palabras clave: Ciber Resiliencia; Ciberseguridad; Comando y Control; Fuerza Aeroespacial; Colombia.

Abstract: This article examines cyber resilience in the command and control centers of the Colombian Aerospace Force, with the objective of identifying strengths and areas for improvement in their capacity to face cyber threats. The study employs a mixed approach, based on a document review, expert interviews and the application of a cyber resilience model and a maturity assessment model adapted to the military context. The results show progress in the management of assets and controls, as well as in the integration of international and national best practices. However, gaps are detected in the formalization of

[1] Mayor de la Fuerza Aeroespacial Colombiana. Candidato a magíster en ciberseguridad y ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ingeniería de Sistemas, Universidad Cooperativa de Colombia, Colombia. https://orcid.org/0009-0009-9303-6523 - Contacto: carlos.uribe@esdeg.edu.co.

continuity and incident recovery plans. In conclusion, strategic and technical guidelines focused on governance, organizational culture, resilient architecture and maturity measurement are proposed in order to strengthen operational sustainability and digital protection in critical environments.

Keywords: Cyber Resilience; Cybersecurity; Command and Control; Aerospace Force; Colombia.

Introducción

En un contexto global marcado por la digitalización acelerada y el auge de las amenazas híbridas, las Fuerzas Armadas enfrentan nuevos desafíos que trascienden el campo físico y se extienden al dominio cibernético. La información se ha consolidado como un recurso crítico y estratégico, especialmente en los Centros de Comando y Control (C2)**,** donde se procesan, comunican y ejecutan decisiones clave para la defensa nacional; a través de una arquitectura compleja compuesta por personas, procedimientos y equipos.

Ante este panorama, garantizar la confidencialidad, integridad y disponibilidad de la información no solo exige robustos esquemas de ciberseguridad (International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC], 2022, p. V), sino también el fortalecimiento de la ciberresiliencia, entendida como la capacidad institucional de anticipar, resistir, recuperarse y adaptarse frente a ciberataques u otras amenazas tecnológicas (Ross et al., 2021, p. 1).

Desde una perspectiva sistémica, los C2 deben ser comprendidos como Sistemas Complejos Adaptativos, por su sigla en inglés CAS (Complex Adaptive System), ya que integran múltiples componentes tecnológicos, humanos, doctrinales y procedimentales que interactúan de forma dinámica, no lineal e interdependiente. Estas características hacen que su comportamiento emergente no pueda explicarse únicamente desde una lógica determinista. Según Holland (1992, p. 19), los CAS poseen tres propiedades fundamentales: evolución, comportamiento agregado y anticipación, lo que les permite reconfigurarse constantemente frente a estímulos externos y mantener patrones de comportamiento persistentes fuera del equilibrio. Esta conceptualización se refuerza con la propuesta de

Carmichael y Hadzikadic (2019, p. 1), quienes destacan que los CAS exhiben autoorganización, retroalimentación correlacionada y capacidad de adaptación colectiva frente a umbrales críticos. Aplicado al entorno militar, ello implica que la resiliencia de los C2 no es un atributo técnico puntual, sino una propiedad emergente del sistema, derivada de su arquitectura distribuida, de sus mecanismos de aprendizaje local y de su robustez organizacional.

Dado este escenario**,** las medidas tradicionales de ciberseguridad, centradas en la prevención y la defensa perimetral, resultan insuficientes frente amenazas cada vez más sofisticadas, persistentes y dinámicas. En consecuencia, se vuelve imprescindible fortalecer la ciberresiliencia, promoviendo una arquitectura organizacional capaz de resistir, recuperarse y garantizar la continuidad operativa incluso en contextos adversos, como ataques intencionales, eventos imprevistos o peligros y sucesos inherentes a infraestructuras críticas, como los C2 (The White House, 2013, p. 12).

En el caso de la Fuerza Aeroespacial Colombiana (FAC), que tienen como misión "volar, entrenar y combatir para vencer y dominar en el aire, el espacio y el ciberespacio, en defensa de la soberanía, la independencia, la integridad territorial, el orden constitucional y contribuir a los fines del Estado" (Fuerza Aérea Colombiana, 2019, p. 2), para el cumplimiento de esta, se ve en la necesidad de evaluar y optimizar sus capacidades de ciberresiliencia en los Centros de Comando y Control de la Fuerza Aeroespacial (CCOFA), dado que estos constituyen puntos neurálgicos en la recolección y fusión de información tanto a nivel estratégico, operacional y táctico, permitiendo la toma de decisiones para la defensa nacional en tiempo real. A su vez, la exposición a ciberamenazas sofisticadas, como ataques persistentes avanzados, por su sigla en inglés APT (Advanced Persistent Threat),

ransomware militarizado, sabotaje digital y manipulación de datos, representa un riesgo creciente que puede comprometer tanto la seguridad informacional como la toma de decisiones operativas críticas (Díaz Mardones, 2021, p. 46).

Aunque la FAC ha implementado esquemas de protección y control en su infraestructura tecnológica, persiste una brecha significativa en la evaluación integral de su resiliencia cibernética. En este escenario, se vuelve prioritario diagnosticar el estado actual de la ciberresiliencia y diseñar estrategias que fortalezcan su capacidad de respuesta ante amenazas emergentes (Aghazadeh Ardebili et al., 2024, p. 4). Por lo tanto, la presente investigación busca responder al siguiente interrogante: ¿Qué lineamientos y tecnologías pueden fortalecer la ciberresiliencia en los centros de comando y control de la FAC frente a amenazas cibernéticas?

La importancia de abordar este problema radica en que los sistemas de C2 militares operan como infraestructuras críticas dentro del ecosistema nacional de defensa. De acuerdo con el Consejo de la Unión Europea (2008, p. 3), se considera infraestructura crítica a todo sistema cuya afectación compromete funciones esenciales para la sociedad y la seguridad del Estado.

Por otra parte, el desarrollo de tecnologías emergentes como el Internet de las Cosas, por su sigla en inglés IoT (Internet of Things), los sistemas ciberfísicos, por su sigla en inglés CPS (Cyber-Physical Systems) y la inteligencia artificial ha incrementado la complejidad de los entornos C2, generando nuevas superficies de ataque y desafíos en la protección de los activos informacionales. Estos entornos hiperconectados, si bien optimizan procesos operativos y de vigilancia, también abren la puerta a ciberamenazas de alta letalidad que pueden alterar el funcionamiento de los sistemas de defensa mediante sabotaje remoto,

espionaje digital o propagación de malware especializado (Djenna et al., 2021; Poulter & Cox, 2021).

Frente a este panorama, esta investigación se orienta a diagnosticar el nivel de ciberresiliencia en los CCOFA, identificar amenazas emergentes que comprometan su operatividad, analizar marcos normativos y tecnológicos aplicables, y formular lineamientos estratégicos ajustados a las particularidades de estos entornos críticos. El enfoque incluye el estudio de capacidades técnicas, organizacionales y doctrinales, en concordancia con los principios de resiliencia cibernética establecidos por el National Institute of Standards and Technology (NIST).

Más allá de un diagnóstico situacional, se busca generar un aporte estructural que consolide la ciberresiliencia como eje transversal de la arquitectura operacional de los CCOFA.

Metodología

Se adopta un enfoque mixto, con preponderancia cualitativa, con el fin de analizar integralmente tanto los aspectos técnicos, estructurales y percepciones institucionales relacionadas con la ciberresiliencia de los CCOFA (Hernández Sampieri et al., 2014, p. 535).

Este estudio tiene un alcance exploratorio y descriptivo, dado que busca comprender el estado actual de la ciberresiliencia en los CCOFA y caracterizar las vulnerabilidades y amenazas emergentes que podrían comprometer la continuidad operacional de los mismos (Hernández Sampieri et al., 2014, p. 90). Así mismo, incorpora un componente propositivo orientado al diseño de lineamientos aplicables de fortalecimiento.

El diseño de investigación es no experimental y de corte transversal, lo que permite recopilar información en un único momento temporal sin manipular variables (Hernández Sampieri et al., 2014, p. 154). Para tal fin, se empleará un modelo de evaluación de madurez de ciberresiliencia adaptado del modelo Revisión de la Ciberresiliencia, por su sigla en inglés CRR (Cyber Resilience Review), desarrollado por el Department of Homeland Security a través de la Cybersecurity and Infrastructure Security Agency (Cybersecurity and Infrastructure Security Agency, 2020), con el objetivo de medir las capacidades organizacionales clave para afrontar incidentes disruptivos.

El análisis cualitativo se desarrolló mediante categorización temática, sustentada en una revisión sistémica de literatura especializada. No obstante, debido al carácter reservado de la información vinculada a procesos críticos de defensa, se profundizó en fuentes normativas, estándares internacionales y marcos doctrinales, enfocados a la ciberresiliencia en infraestructuras críticas. En el componente cuantitativo, se aplicó estadística descriptiva para interpretar los datos recolectados a través de entrevistas a profundidad realizadas a personal militar y técnico con funciones directas en ciberseguridad, ciberdefensa, seguridad informática y gestión de riesgos dentro de los CCOFA (Hernández Sampieri et al., 2014, p. 534). La triangulación metodológica se realizó integrando los hallazgos teóricos, las percepciones institucionales obtenidas mediante entrevistas a profundidad y los resultados cuantitativos derivados del modelo de revisión del nivel de madurez de ciberresiliencia. Esto fortaleció la rigurosidad del diagnóstico y sustentó el diseño de la propuesta, la cual fue validada mediante el método DELPHI a través de un panel de tres expertos con la experticia y pertinencia requeridas.

Desde el punto de vista ético, la investigación garantiza el consentimiento informado de los participantes, el respeto a la confidencialidad de los datos y el cumplimiento de las directrices institucionales en cuanto a la aprobación del estudio y el manejo seguro de la información sensible.

Fundamentos conceptuales de la ciberresiliencia

La ciberresiliencia constituye un enfoque integral que trasciende los límites de la ciberseguridad tradicional centrada exclusivamente en la prevención. Su adecuada comprensión requiere el análisis de su definición y evolución conceptual, así como sus diferencias con respecto a la ciberseguridad y la ciberdefensa. Además, implica examinar sus objetivos funcionales, su aplicación estratégica en infraestructuras críticas y los principios de ingeniería que fundamentan el diseño de sistemas resilientes.

Definición y evolución del concepto de ciberresiliencia

La ciberresiliencia ha emergido como una evolución necesaria ante la creciente sofisticación de las amenazas cibernéticas y la evidente insuficiencia de los enfoques tradicionales de ciberseguridad, los cuales se han centrado exclusivamente en la prevención y protección. Para comprender adecuadamente este concepto, es fundamental partir de su base teórica: La resiliencia se puede caracterizar desde múltiples puntos de vista, incluida la capacidad de un sistema para absorber las perturbaciones o el grado de perturbación que puede soportar antes de que el sistema experimente alteraciones estructurales mediante la modificación de las variables y los procesos que dictan su funcionamiento (Tzavara & Vassiliadis, 2024, p. 1698).

La resiliencia es un concepto multifacético ampliamente examinado en varios campos científicos, como la psicología, la sociología, la ecología y la ingeniería, interpretado de

manera consistente como la capacidad de anticipar y adaptarse a las posibles amenazas, lo que refleja una capacidad dinámica de respuesta.

En esta línea, la ciberresiliencia hereda el principio adaptativo de la resiliencia tradicional, pero lo articula desde una perspectiva operativa. Ross et al. (2021) define la ciberresiliencia como:

> La capacidad de anticipar, resistir, recuperarse y adaptarse a condiciones adversas, tensiones, ataques o compromisos en sistemas que utilizan o están habilitados por recursos cibernéticos. La resiliencia cibernética tiene como fin permitir que los objetivos de la misión o de negocio que dependen de los recursos cibernéticos se logren en un entorno conflictivo. (p. 76)

Para comprender cómo se ha llegado a esta concepción, resulta esencial examinar la evolución progresiva del concepto, la cual ha seguido un desarrollo cronológico estructurado en tres etapas:

- **Antes de 2002**: Surgimiento de las primeras preocupaciones sobre resiliencia en entornos digitales.
- **2003-2010**: Consolidación del interés académico e institucional, con un enfoque más profundo en los fundamentos teóricos y aplicaciones prácticas.
- **2011-2019**: Notable aumento de la producción científica y establecimiento de marcos conceptuales contemporáneos, reflejando la maduración del campo y la complejidad de las amenazas emergentes.

Esta progresión cronológica no solo facilita una comprensión más profunda de la naturaleza transformadora del enfoque resiliente en el contexto del ciberespacio, sino que

también establece una base fundamental para los estudios prospectivos que buscan explorar los cambios estructurales provocados por eventos disruptivos globales, como el inicio de la pandemia de COVID-19 que comenzó en el año 2020 (Tzavara & Vassiliadis, 2024, pp. 1698-1699).

En este contexto, es imperativo delinear conceptualmente la ciberresiliencia en relación con los conceptos asociados, como la ciberseguridad y la ciberdefensa, a fin de articular sus parámetros operativos en entornos dinámicos y profundamente interconectados.

Diferencias entre ciberresiliencia, ciberseguridad y ciberdefensa

En el ámbito cibernético, es fundamental distinguir entre los conceptos de ciberseguridad, ciberresiliencia y ciberdefensa, dado que, aunque relacionados, responden a enfoques y alcances diferenciados. La ciberseguridad se enfoca primordialmente en prevenir y mitigar amenazas relacionadas con el acceso no autorizado, mediante la implementación de controles técnicos, políticas de protección y mecanismos de respuesta ante incidentes. Su orientación es principalmente preventiva y correctiva, orientada a evitar la explotación de vulnerabilidades por parte de actores tanto internos como externos. Por su parte, la ciberresiliencia representa un enfoque más amplio e integrador, que no solo contempla la prevención y protección, sino que se centra en garantizar la continuidad operativa de las funciones críticas de la organización, incluso ante incidentes exitosos de seguridad. Este paradigma promueve la capacidad de anticipar, resistir, recuperarse y adaptarse frente a perturbaciones, permitiendo que las misiones se mantengan funcionales en entornos cibernéticos adversos (Conklin & Shoemaker, 2017, p. 15).

En complemento, la ciberdefensa adopta una perspectiva basada en principios doctrinales militares, en la cual se integran capacidades y procesos sincronizados en tiempo

real para detectar, analizar y mitigar amenazas cibernéticas, con el propósito de superar en maniobras a actores adversarios y proteger redes y misiones críticas. Esta concepción se estructura en tres niveles: el estratégico, el operativo y el táctico. En conjunto, estos niveles conforman un escudo de ciberdefensa que articula capacidades defensivas y ofensivas, fundamentales para operar eficazmente en entornos digitales hostiles y tecnológicamente complejos (de Nobrega et al., 2024, p. 2).

Sin embargo, para fortalecer aún más la seguridad y resiliencia de estos sistemas, resulta indispensable conocer los marcos y estándares internacionales de ciberresiliencia, los cuales ofrecen lineamientos técnicos y regulatorios que complementan y potencian las capacidades defensivas existentes.

Marcos y estándares internacionales de ciberresiliencia

La ciberresiliencia ha sido abordada desde múltiples marcos regulatorios y técnicos reconocidos internacionalmente. Entre los más relevantes destacan:

- **Cyber Resilience Act (CRA)** propuesto por la Unión Europea, que establece requisitos regulatorios para productos digitales y componentes críticos (European Commission, 2022).
- **Cybersecurity Assessment Framework (CAF)** del National Cyber Security Centre del Reino Unido, que permite evaluar de forma estructurada la postura de seguridad de organizaciones esenciales (National Cyber Security Centre, 2024).
- **Cyber Resiliency Engineering Framework (CREF)** desarrollado por MITRE, que define principios de diseño resiliente desde la fase de arquitectura de sistemas (Bodeau et al., 2011).

- **Cyber Resiliency Level (CRL)** propuesto por Lockheed Martin, que permite categorizar el nivel de resiliencia de una organización en función de sus capacidades (Cyber resiliency level®, n.d.).
- **Cyber Resilience Index and Framework** del World Economic Forum, que promueve indicadores estandarizados para comparar la resiliencia digital a nivel global (World Economic Forum, 2022).
- **NIST SP 800-160 Vol. 2** desarrollado por el Instituto Nacional de Estándares y Tecnología de EE.UU., que proporciona un enfoque integral para diseñar y mantener sistemas confiables, seguros y resilientes en ambientes críticos (Ross et al., 2021).

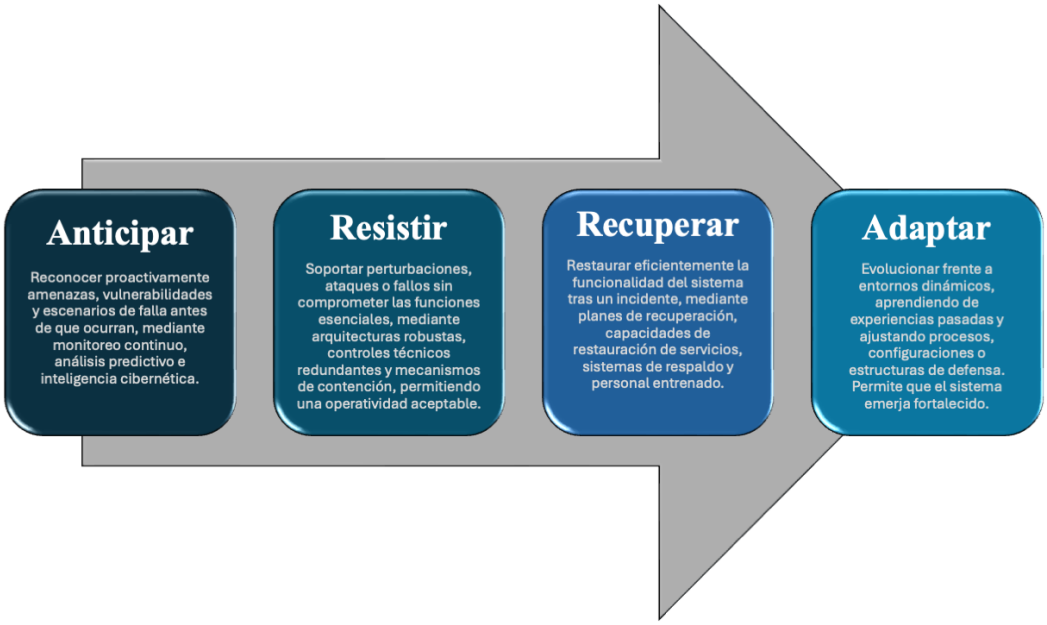
Aunque todos estos marcos ofrecen enfoques válidos y complementarios, esta propuesta adopta como eje estructural el marco NIST SP 800-160 Vol. 2, dado su enfoque técnico y sistémico para el diseño y mantenimiento de sistemas resilientes frente a ciberamenazas. Además, su compatibilidad con el modelo Cyber Resilience Review (CRR) del Departamento de Seguridad Nacional de Estados Unidos, por su sigla en inglés DHS (U.S. Department of Homeland Security) y su orientación hacia sistemas complejos adaptativos (CAS) y entornos críticos lo hacen especialmente adecuado para su aplicación en entornos militares como los CCOFA.

Esta elección responde a la necesidad de contar con un marco de referencia que integre dimensiones técnicas, organizacionales y operativas, favoreciendo la implementación progresiva de prácticas resilientes alineadas con los objetivos de defensa nacional. En este sentido, es indispensable identificar las metas resilientes que sustenten este marco de referencia.

Metas resilientes: anticipar, resistir, recuperarse y adaptarse

Una vez establecidos los fundamentos conceptuales de la ciberresiliencia y sus distinciones frente a la ciberseguridad y la ciberdefensa, junto con los diferentes marcos y estándares internacionales, resulta pertinente profundizar en los principios operativos que guían su implementación en entornos críticos como los CCOFA. En este contexto, el marco de referencia propuesto por el NIST Special Publication 800-160 Vol. 2 adquiere especial relevancia, al estructurar la resiliencia cibernética en torno a cuatro metas fundamentales: anticipar, resistir, recuperarse y adaptarse. Estos pilares orientan el diseño de sistemas capaces de mantener su funcionalidad frente a condiciones adversas, permitiendo a las organizaciones sostener sus misiones esenciales incluso ante ataques o fallas (Ross et al., 2021, p. 1). La Figura 1 presenta una visualización secuencial de las metas fundamentales de la ciberresiliencia y su relevancia en los contextos definidos como CAS.

Figura 1. Metas fundamentales ciberresiliencia



Fuente: elaboración propia basado en la información obtenida por Ross et al. (2021, p. 10)

En conjunto, estas metas constituyen la base operativa del enfoque resiliente, permitiendo que los sistemas críticos no solo sobrevivan a los incidentes, sino que mejoren continuamente frente a un entorno cibernético cada vez más hostil e impredecible, siendo relevante en escenarios donde los impactos pueden comprometer la continuidad del Estado, la defensa nacional o la integridad de infraestructuras vitales.

Ciberresiliencia como estrategia operativa en infraestructuras críticas

A partir de las metas descritas, resulta clave comprender cómo se articulan de manera operativa en contextos de alta criticidad. Las infraestructuras críticas, por su dependencia tecnológica y su papel estratégico para la seguridad y el bienestar nacional, requieren modelos de gestión cibernética que integren la resiliencia como eje transversal.

En este sentido, la acelerada digitalización de las infraestructuras críticas ha incrementado de manera significativa la necesidad de adoptar estrategias de ciberresiliencia que superen los enfoques tradicionales, centrados exclusivamente en la protección y la respuesta reactiva ante incidentes. Estas infraestructuras, incluyendo los sistemas de energía, transporte, agua, salud, telecomunicaciones y, de manera destacada, los C2 en el ámbito militar, constituyen pilares fundamentales del funcionamiento socioeconómico y estratégico de los Estados. Su vulnerabilidad ante ciberamenazas representa un riesgo con potenciales consecuencias a nivel nacional y transnacional (Araujo et al., 2024, p. 5)

Conforme a la Directiva Presidencial de Política 21 (PPD-21) de los Estados Unidos, se entiende por infraestructura crítica todo sistema o activo, físico o virtual, que sea vital para una nación y cuya interrupción o destrucción podría tener un impacto debilitante en la seguridad nacional, economía, salud pública o cualquier combinación de estos aspectos (The White House, 2013, p. 12). Esta definición da una alta importancia a la interdependencia

sectorial y la necesidad de adoptar abordajes integrales que consideren la convergencia entre los espacios físico y digital.

En consonancia con lo anterior, Araujo et al. (2024) advierten que los CPS integrados en infraestructuras críticas presentan riesgos significativos debido a la interacción compleja entre sus componentes computacionales, comunicacionales y físicos. Esta condición demanda una concepción holística de la ciberresiliencia, que complemente los mecanismos de seguridad tradicional con capacidades adaptativas, preventivas y de recuperación (p. 5). En este contexto, la ciberresiliencia emerge como un componente esencial para preservar la continuidad funcional de dichos sistemas frente a eventos disruptivos.

En entornos militares, la necesidad de fortalecer la ciberresiliencia cobra aún mayor relevancia. La dependencia de infraestructuras críticas para la ejecución de misiones y la protección de la soberanía nacional hace que cualquier vulnerabilidad represente una amenaza directa a la seguridad del Estado. Tal como lo advierte Bagrodia (2022, pp. 97–98), el Departamento de Defensa de Estados Unidos ha priorizado la resiliencia cibernética como una línea estratégica para garantizar la operatividad de sus sistemas de información y armas ante potenciales ataques. Esta preocupación se magnifica en sistemas altamente integrados, cuya funcionalidad depende de una red interconectada de sensores, plataformas y sistemas de armas, lo cual significa, que una interrupción en estos sistemas puede generar fallos operacionales en cadena, subrayando la urgencia de contar con capacidades resilientes que aseguren la continuidad de la misión.

En este marco, los C2 del ámbito militar se reconocen como infraestructuras críticas altamente sensibles, pues concentran capacidades decisionales, operativas y de comunicación que soportan el mando estratégico y la defensa nacional. Desde un enfoque sistémico,

garantizar la ciberresiliencia de los C2 representa no solo una necesidad táctica, sino también un imperativo estratégico, ya que estos nodos funcionales articulan capacidades clave para la gestión de crisis, el despliegue operacional y la protección de activos esenciales. En consecuencia, el fortalecimiento de la ciberresiliencia en los C2 se constituye en el objetivo central, al considerar que su estabilidad y adaptabilidad determinan en gran medida la efectividad de la respuesta institucional ante amenazas avanzadas y persistentes.

En síntesis, esta visión se presenta como una condición necesaria para enfrentar los desafíos emergentes de un entorno digital dinámico, incierto y cada vez más hostil, y se establece como punto de partida para el análisis de los principios de diseño ciberresiliente contenidos en el marco técnico seleccionado.

Principios de diseño resiliente según el marco NIST SP 800-160 Vol. 2

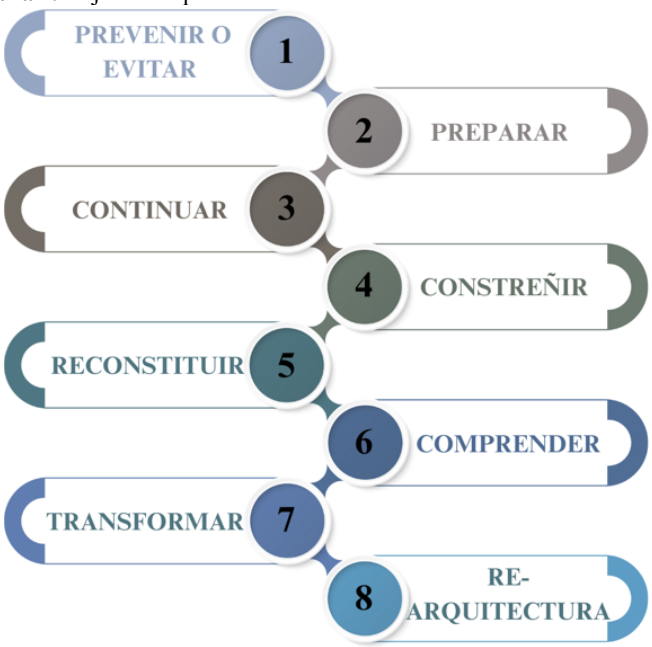
En el ámbito de las infraestructuras críticas militares, los C2 ocupan un lugar estratégico por su función en la coordinación operativa, la ejecución táctica y la toma de decisiones a nivel nacional. Esta condición impone la necesidad de incorporar principios de diseño resiliente en su arquitectura y operación, con el fin de garantizar su funcionalidad continua incluso bajo condiciones extremas de adversidad cibernética. El marco normativo propuesto por el NIST en la publicación especial SP 800-160 Vol. 2 proporciona directrices fundamentales para el desarrollo de sistemas ciberresilientes que aseguren la misión en entornos operativos hostiles.

Este marco de referencia, titulado Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, establece que los sistemas críticos deben ser diseñados con la capacidad de anticipar, resistir, recuperarse y adaptarse frente a ataques cibernéticos, sin comprometer sus funciones esenciales (Ross et al., 2021, p. 1), tal como se explicó previamente. Esta perspectiva se fundamenta en una aproximación sistémica orientada a

preservar las funciones de misión, más allá de simplemente prevenir fallos. En consecuencia, la ciberresiliencia se concibe como una propiedad emergente del sistema, desarrollada a partir de la integración deliberada de técnicas específicas y principios de diseño a lo largo de todo su ciclo de vida (Ross et al., 2021, pp. 2–3).

Como complemento a estas cuatro metas funcionales, el marco introduce ocho objetivos específicos de ciberresiliencia, descritos en la Figura 2, que orientan la implementación técnica de estas capacidades y fortalecen su aplicación en entornos operativos.

Figura 2. Objetivos específicos de ciberresiliencia



Fuente: elaboración propia basado en la información obtenida por Ross et al. (2021, pp. 10-12) y traducida al español

Estos objetivos funcionan como principios orientadores y adaptativos que permiten construir sistemas robustos personalizados, capaces de sostener y garantizar su misión frente a condiciones inciertas o hostiles (Ross et al., 2021, pp. 10-12).

Para alcanzar estas metas y objetivos, el NIST SP 800-160 Vol. 2 propone una combinación de 14 técnicas y 49 enfoques que integran principios de ingeniería de sistemas

seguros con gestión del riesgo (Ross et al., 2021, pp. 12-14). Tal cual como se describe en la Figura 3 a continuación:

Figura 3. Técnicas de ciberresiliencia y enfoques de aplicación

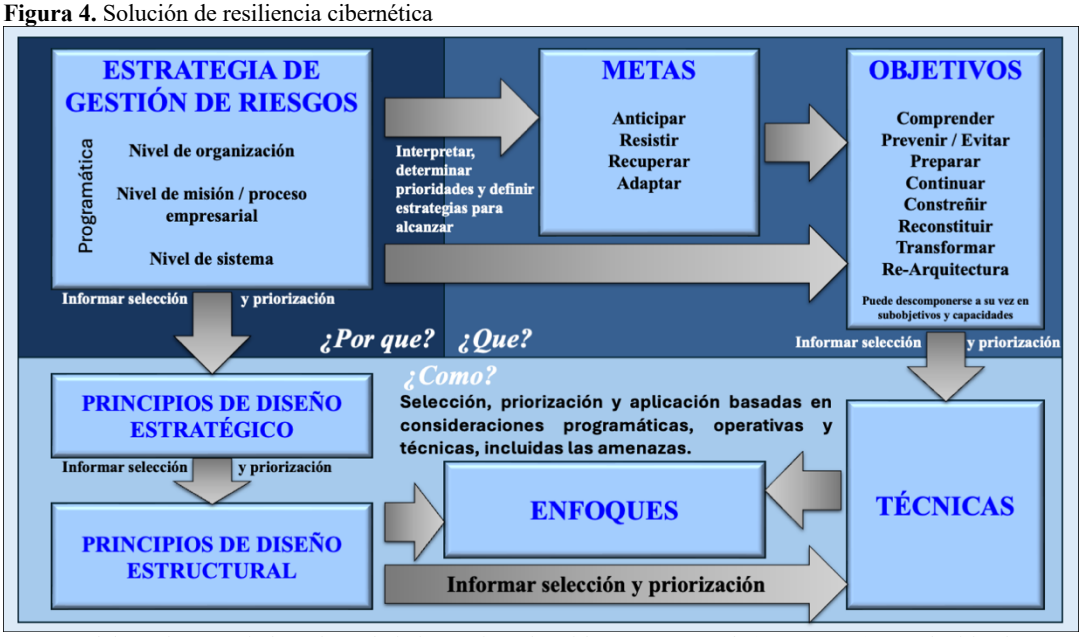
Fuente: elaboración propia basado en la información obtenida por Ross et al. (2021, pp. 12-14) y traducida al español

La integración de estas técnicas y enfoques contribuye a crear un ecosistema técnico y organizacional resiliente, adaptable y sostenible frente a amenazas dinámicas.

Para llevar a la práctica esta estructura, el NIST sugiere una secuencia metodológica lógica y adaptable. El proceso inicia con la evaluación del entorno estratégico y los requerimientos de misión del sistema en cuestión. Luego, se identifican y priorizan los objetivos resilientes más pertinentes, en función del perfil de amenazas y de los riesgos previamente identificados. A partir de esta priorización, se seleccionan los enfoques técnicos y las técnicas más apropiadas que respondan a las características específicas de la arquitectura, el contexto operativo y las restricciones del sistema (Ross et al., 2021, pp. 8-16).

En este mismo sentido, el marco NIST SP 800-160 Vol. 2 proporciona una estructura clara que orienta el diseño de sistemas ciberresilientes. Esta se construye sobre tres preguntas clave: el ¿qué? (los resultados resilientes esperados), el ¿cómo? (los mecanismos para alcanzarlos) y el ¿por qué? (el contexto organizacional y de riesgo que justifica su integración), tal como se presenta en la Figura 4 (Ross et al., 2021, pp. 8-16).

Figura 4. Solución de resiliencia cibernética



Fuente: elaboración propia basado en la información obtenida por Ross et al. (2021, p. 16) y traducida al español

En síntesis, este marco de referencia no solo ofrece una taxonomía robusta de técnicas y objetivos resilientes, sino que establece una lógica operativa coherente para su integración en entornos altamente críticos como los CCOFA. Este enfoque transforma el diseño resiliente en una capacidad estratégica que permite garantizar el éxito de la misión incluso ante escenarios disruptivos y persistentes.

Finalmente, teniendo claro los fundamentos establecidos por el NIST SP 800-160 Vol. 2, el siguiente apartado abordará de forma general el estado actual de la ciberresiliencia en los CCOFA.

Diagnóstico de ciberresiliencia en entornos militares

La evaluación de la ciberresiliencia en entornos militares representa un paso crítico para determinar el grado de preparación y adaptación de los sistemas ante amenazas avanzadas y escenarios operativos adversos. Este diagnóstico permite identificar tanto las fortalezas como las brechas existentes en la implementación de capacidades resilientes, ofreciendo una visión integral sobre el estado actual de protección y continuidad en infraestructuras críticas. En particular, el análisis se centrará en los CCOFA, considerados núcleos funcionales de alto valor operativo.

Desde una perspectiva de sistemas, tal cual se hace referencia en la introducción, los CCOFA pueden conceptualizarse como CAS, tal como lo establece Acur y Hendriks (2024, p. 480), quienes argumentan que estos sistemas, al operar en contextos digitales y con alta interconectividad, enfrentan riesgos emergentes que requieren enfoques de ciberresiliencia transversales y sistémicos.

A lo largo de esta sección, se abordarán elementos clave como las funciones críticas que estos desempeñan, el modelo de evaluación disponible, los indicadores esenciales de resiliencia y el nivel de madurez organizacional y técnica frente a las exigencias del entorno.

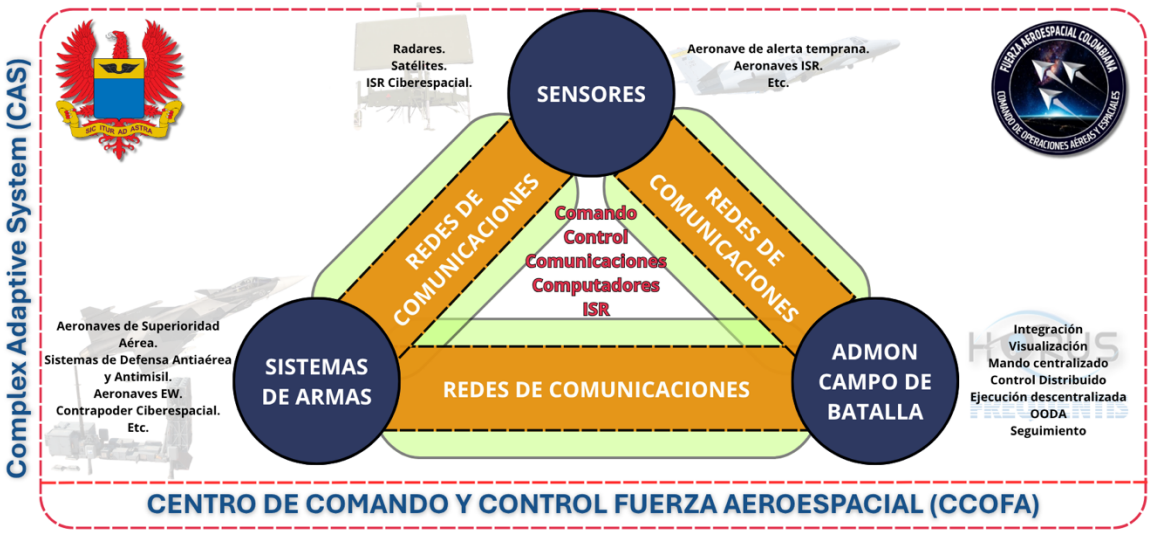
Funciones críticas de los CCOFA

Los C2 constituyen el eje operacional de las fuerzas armadas modernas, integrando, procesando y distribuyendo información crítica para la toma de decisiones estratégicas, tácticas y logísticas. Actuando como núcleos tecnológicos y estratégicos que consolida los elementos operativos de las fuerzas militares (plataformas, personal, armamento y recursos adicionales) con capacidades de inteligencia, redes tácticas e instrumentos analíticos. Esta

sinergia proporciona al mando militar un conocimiento situacional en tiempo real y una evaluación predictiva que optimiza la eficiencia en la toma de decisiones (Baesystems.com, s.f.).

En este contexto, los CCOFA pueden entenderse como estructuras altamente integradas que combinan sensores para la adquisición de información, plataformas computacionales para el análisis de datos y redes de comunicación para una difusión eficiente de la información, como se ilustra en la Figura 5.

Figura 5. Arquitectura CCOFA



Fuente: elaboración propia basado en las entrevistas

La estructura anterior, no solo describe los componentes técnicos y funcionales que conforman los CCOFA, sino que también permite comprender cómo se articulan sus capacidades en un entorno operacional concreto. A partir de esta arquitectura, es posible evidenciar cómo dichas capacidades se traducen en ventajas estratégicas dentro del ámbito militar, especialmente en la gestión y ejecución de operaciones aéreas.

Figura 6. Capacidades operacionales CCOFA

Fuente: elaboración propia basada en la experiencia

Desde el punto de vista operacional, y como se muestra en la Figura 6, en el caso de la FAC, los CCOFA son responsables tanto de mantener una supervisión centralizada de las operaciones aéreas como de apoyar la ejecución eficiente y descentralizada de las misiones asignadas. Este principio del poder aéreo y espacial reviste gran relevancia, ya que permite aprovechar la velocidad y versatilidad de las aeronaves para concentrar las fuerzas en maniobras ofensivas o defensivas de forma oportuna. Asimismo, facilita, conforme a la planificación estratégica, la identificación y priorización de objetivos dentro del teatro de operaciones, con el propósito de establecer un equilibrio adecuado y garantizar una capacidad de ataque sostenida (Fuerza Aérea Colombiana, 2013, p. 62).

Dado su carácter crítico, cualquier interrupción, degradación o vulnerabilidad en estos sistemas podría comprometer seriamente la capacidad de respuesta institucional. Esta necesidad da paso al análisis de modelos estandarizados que orienten dicha evaluación de manera estructurada y cuantitativa.

Modelo de evaluación de resiliencia: Cyber Resilience Review (CRR)

Este es un modelo de evaluación de ciberresiliencia desarrollada por el Departamento de Seguridad Nacional de Estados Unidos (DHS) y administrado por la Agencia de Seguridad de Infraestructura y Ciberseguridad, por su sigla en inglés CISA (Cybersecurity and Infrastructure Security Agency) (CISA, 2020, p. 1). Este modelo se fundamenta en el Resilience Management Model (RMM), que fue formulado por la División CERT del Instituto de Ingeniería de Software de la Universidad Carnegie Mellon en Pittsburgh, Pensilvania – EEUU (CISA, 2020, p. 3). Con el objetivo de proporcionar una evaluación estandarizada del nivel de madurez en ciberresiliencia en organizaciones críticas. Su propósito es identificar qué tan preparados están sus procesos para enfrentar amenazas cibernéticas, midiendo su capacidad para manejar riesgos, mantener sus operaciones clave durante un ataque y recuperarse de forma rápida y efectiva (CISA, 2020, p. 1).

Lo anterior, se soporta en un proceso evaluativo basado en entrevistas estructuradas, destinado a evaluar el marco de gestión de la ciberseguridad de una organización. Su finalidad es obtener información sobre la gestión de los servicios de ciberseguridad y sus activos pertinentes, que son cruciales para el cumplimiento exitoso de los objetivos de una organización. Haciendo hincapié en las estrategias de protección y mantenimiento en los ámbitos críticos que mejoran la ciberresiliencia integral de una organización. Ofreciendo métricas significativas sobre la resiliencia operativa de una organización, tanto durante las actividades rutinarias como en los períodos de adversidad operativa (CISA, 2020, p. 3).

Figura 7. Dominios modelo CRR

Fuente: elaboración propia basado en la información obtenida por CISA (2020, p. 4) y traducida al español

Como se observa en la Figura 7, el modelo se estructura en torno a diez dominios fundamentales, cada uno de estos se analiza a través de prácticas específicas que se cuantifican mediante un Nivel Indicador de Madurez (MIL), los cuales comprenden seis escalas: incompleto (MIL0), realizado (MIL1), planificado (MIL2), gestionado (MIL3), medido (MIL4) y definido (MIL5). Esta clasificación permite a la organización discernir sus fortalezas, debilidades y rutas de mejora continua en la implementación de capacidades de ciberresiliencia (CISA, 2020, pp. 16-17).

Este modelo resulta útil para utilizarlo en entornos como los CCOFA, ya que ofrece una metodología estructurada y flexible para evaluar su capacidad de anticipar, resistir, recuperar y adaptarse frente a amenazas complejas. Además, su enfoque no invasivo y de bajo costo lo convierte en una opción práctica para implementar en infraestructuras criticas militares, donde mantener la continuidad operativa es fundamental. En este sentido, resulta

pertinente examinar con mayor detalle los dominios fundamentales del modelo CRR, los cuales constituyen el núcleo de su enfoque diagnóstico y permiten una evaluación del nivel de ciberresiliencia organizacional.

Análisis dominios fundamentales modelo CRR

A continuación, se presenta una descripción detallada de estos dominios:

- **Gestión de activos**: Identificación, registro y administración de recursos esenciales (personal, información, tecnología, instalaciones) (CISA, 2020, p. 5).
- **Gestión de controles**: Identificación, análisis y administración de controles para lograr objetivos y asegurar la mejora continua (CISA, 2020, pp. 6-7).
- **Gestión de configuraciones y cambios**: Protección de la integridad de los activos mediante controles y auditorías, minimizando riesgos de modificaciones (CISA, 2020, p. 8).
- **Gestión de vulnerabilidades**: Identificación, análisis, gestión y control de vulnerabilidades para prevenir interrupciones, anticipando amenazas (CISA, 2020, p. 9).
- **Gestión de incidentes**: Creación de procedimientos para identificar, analizar y responder a eventos e incidentes (CISA, 2020, p. 10).
- **Gestión de continuidad del servicio**: Asegurar que operaciones y activos esenciales sigan funcionando ante incidentes o desastres, mediante planes de respuesta (CISA, 2020, p. 10).

- **Gestión de Riesgos**: Identificación, análisis y mitigación de amenazas que puedan afectar activos y servicios críticos, centrándose en riesgos cibernéticos (CISA, 2020, p. 12).
- **Gestión de servicios externos**: Establecimiento de controles para proteger servicios y activos que dependen de terceros (CISA, 2020, p. 13).
- **Concientización y entrenamiento**: Promoción del conocimiento y cumplimiento de los objetivos de ciberresiliencia de la organización por parte del personal (CISA, 2020, p. 14).
- **Conciencia y situacional**: Recopilación y distribucion de información precisa sobre la estabilidad y seguridad operativa para una visión común (CISA, 2020, p. 14).

Al analizar estos dominios, es posible identificar con claridad tanto las fortalezas como las áreas que requieren mejora, lo cual permite definir estrategias que se ajustan realmente a las necesidades operativas y al enfoque de diseño resiliente que propone el marco NIST SP 800-160 Vol. 2.

Evaluación de madurez de los CCOFA

Se llevó a cabo un ejercicio de evaluación de madurez de Ciberresiliencia aplicado a los CCOFA. Para ello, se diseñó y aplicó un cuestionario estructurado con preguntas cerradas, administrado mediante una entrevista a profundidad que abarcó los 10 dominios definidos por el modelo CRR. Este instrumento fue aplicado a cuatro oficiales expertos de la FAC, responsables de las áreas de ciberseguridad y ciberdefensa, así:

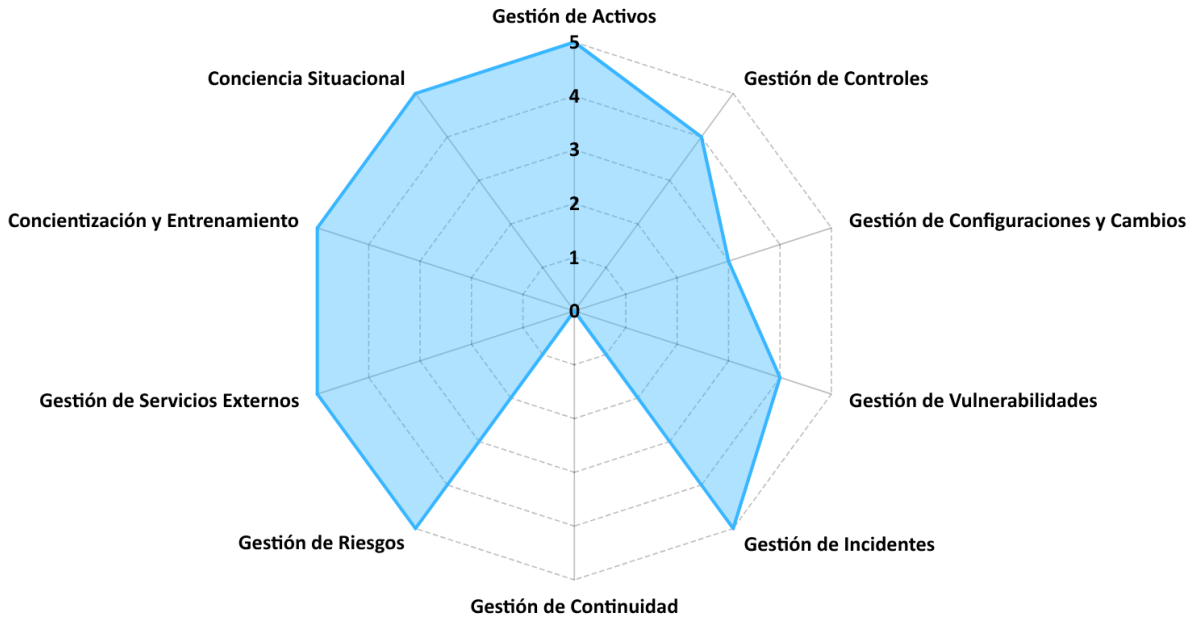
- **Director Cibernética, Aérea y Espacial** (DICAE).
- **Subdirector Ciberdefensa Aérea** (DICAE-SUCDA).

- **Director Seguridad Informática y Electrónica** (DISIE).
- **Subdirector Gestión de Riesgos Tecnológicos** (DISIE-SUGET).

Las entrevistas a profundidad permitieron obtener insumos cualitativos y cuantitativos sobre la percepción y nivel de implementación de prácticas resilientes en los CCOFA. Cada respuesta fue tabulada y cuantificada bajo el sistema de Niveles Indicadores de Madurez (MIL).

A continuación, en la Figura 8 se presentan los resultados obtenidos

Figura 8. Nivel de madurez (MIL) por dominio



Fuente: elaboración propia, con Excel, basado en la tabulación de las entrevistas a profundidad

Desde el punto de vista cuantitativo, el nivel de ciberresiliencia de los CCOFA, basado en el modelo CRR, es de 4 sobre 5. Un promedio en MIL 4 indica que la Fuerza Aeroespacial Colombiana, posee una alta madurez en ciberresiliencia**,** con mecanismos formales para medir y mejorar continuamente sus capacidades de protección, respuesta y recuperación ante amenazas cibernéticas.

Como resultado, se identificó una brecha critica en la ciberresiliencia de los CCOFA, en el dominio de Gestión de Continuidad. Debido a que no existen planes de continuidad del negocio documentados, como son el **Plan de Recuperación ante Desastres**, por su sigla en inglés DRP (Disaster Recovery Plan) y el **Plan de Continuidad del Negocio**, por su sigla en inglés BCP (Business Continuity Plan). El DRP se enfoca en restaurar sistemas de Tecnologías de la Información (TI) tras desastres, mientras el BCP asegura la continuidad integral del negocio durante interrupciones significativas. Esta deficiencia limita la capacidad institucional para reaccionar de manera sistemática ante eventos imprevistos, consolidando una oportunidad de mejora prioritaria en el marco de la ciberresiliencia organizacional (CISA, 2020, p. 11).

En consecuencia, es esencial fortalecer los marcos de continuidad y recuperación como un componente fundamental de una estrategia de ciberresiliencia, particularmente cuando nos enfrentamos a un entorno digital cada vez más complejo. Bajo esta conclusión, el análisis de amenazas cibernéticas emergentes se convierte en el siguiente punto crítico para comprender la evolución del riesgo en entornos militares complejos y diseñar respuestas estratégicas más eficaces.

Amenazas cibernéticas emergentes

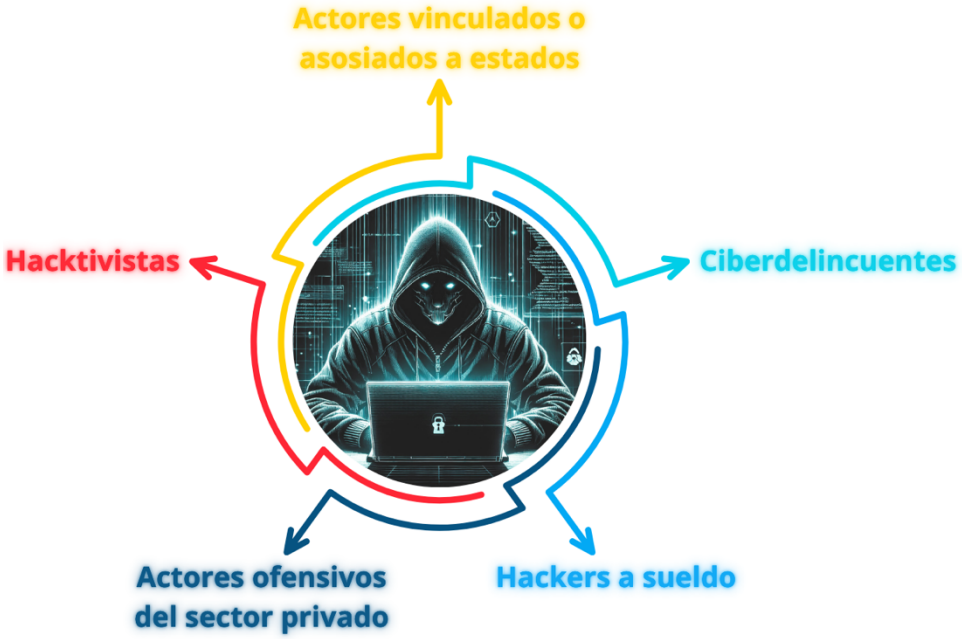
Los CCOFA son infraestructuras militares críticas cuya continuidad operativa es fundamental para la defensa. Sin embargo, el panorama de amenazas cibernéticas evoluciona constantemente en complejidad e intensidad, poniendo en riesgo estos entornos. Actores hostiles, desde grupos delictivos hasta agencias estatales, llevan a cabo campañas avanzadas de espionaje, sabotaje y desestabilización mediante ataques persistentes y sofisticados. En

este apartado se analizan las principales amenazas cibernéticas emergentes enfocadas en los CCOFA y seguidas por la importancia de la inteligencia de amenazas ciberneticas. Asimismo, se discuten los riesgos que dichas amenazas suponen para los principios básicos de seguridad de la informacion, Confidencialidad, Integridad y Disponibilidad, por su sigla en inglés CIA (Confidentiality - Integrity - Availability), en entornos de C2, y se presentan casos documentados a nivel internacional que ilustran el impacto real de estas ciberamenazas en sistemas militares e infraestructuras criticas de algunos paises.

Tipos de amenazas relevantes para infraestructuras militares

Para comprender el alcance de las amenazas cibernéticas que enfrentan infraestructuras críticas como los CCOFA, es esencial identificar primero su origen. Según la European Union Agency for Cybersecurity (ENISA, 2024, p. 4), los principales actores responsables de estas amenazas se agrupan en cuatro categorías, como se ilustra en la Figura 9 a continuación:

Figura 9. Principales actores responsables de amenazas Cibernéticas



Fuente: elaboración propia basado en la información obtenida por ENISA (2024, p. 4)

Cada uno de estos actores responde a motivaciones distintas, como el espionaje, el beneficio económico, la desestabilización estratégica o el activismo político. Esta diversidad amplía el espectro y el alcance de los riesgos que enfrentan las infraestructuras críticas militares.

Dado que estas amenazas provienen de actores tan variados y sofisticados, su identificación debe ser sistemática y considerar el impacto específico sobre los entornos militares. Por ello, es fundamental clasificar no solo su tipología técnica, sino también los vectores de ataque más utilizados, las tácticas y técnicas asociadas, desde el marco MITRE ATT&CK, y su afectación directa sobre los sistemas estratégicos.

La siguiente tabla resume las amenazas cibernéticas más relevantes para entornos militares como los CCOFA. La selección de estas amenazas se realizó a partir de una revisión documental especializada, basada en publicaciones científicas, marcos técnicos reconocidos (MITRE ATT&CK, ENISA y World Economic Forum) y casos documentados de impacto en infraestructuras militares críticas. Se priorizaron aquellas amenazas con mayor frecuencia, impacto operacional y aplicabilidad al entorno de los C2. La clasificación se estructuró según el marco MITRE ATT&CK, lo cual permitió vincular tácticas y técnicas con consecuencias observadas en escenarios reales.

Tabla 1. Amenazas cibernéticas más relevantes

Tipo de amenaza	Descripción breve	Táctica MITRE ATT&CK	Técnica MITRE ATT&CK	Impacto sobre los CCOFA	Ejemplo documentado
Ataque a la cadena de suministro	Compromiso de software y hardware confiable para acceder a redes críticas.	Acceso inicial	T1195.002 (Comprometer la cadena de suministro de software) T1195.003 (Comprometer la cadena de suministro de hardware)	Espionaje prolongado, acceso privilegiado, mapeo de redes militares y eventualmente control sobre sistemas críticos.	Caso SolarWinds (EE. UU., 2020)

Tipo de amenaza	Descripción breve	Táctica MITRE ATT&CK	Técnica MITRE ATT&CK	Impacto sobre los CCOFA	Ejemplo documentado
Ransomware dirigido	Encriptación de sistemas críticos y demanda de rescate.	Impacto	T1486 (Datos encriptados para impacto)	Paralización de operaciones críticas e indisponibilidad de datos estratégicos.	Caso Irish Health Service Executive (Irlanda, 2021)
APT (Amenaza Persistente Avanzada)	Infiltración prolongada mediante múltiples vectores.	Exfiltración	T1041 (Exfiltración por canal de red)	Acceso a redes internas, espionaje continuo y exfiltración de información clasificada.	APT29 Caso SolarWinds (EE. UU., 2020)
Ataques DDoS	Saturación de servicios mediante tráfico masivo.	Impacto	T1498 (Denegación de Servicio de Red) T1499 (Denegación de Servicio en Endpoint)	Inhabilitación de redes de comunicación de comando, afectando la coordinación de misiones.	Ataque DDoS a organismos de defensa de Ucrania (2022)
Sabotaje cibernético	Manipulación de sistemas para provocar fallos físicos o lógicos.	Impacto	T1561 (Borrad de disco) T1565 (Manipulación de datos) T1489 (Parada del Servicio) T1490 (Inhibir la recuperación del sistema) T1529 (Apagado/Reinicio del Sistema)	Alteración de sistemas de control operacional y pérdida de confianza en plataformas militares.	Stuxnet en plantas nucleares iraníes (2010)
Ataques IoT militares	Explotación de dispositivos conectados como sensores.	Impacto	T1495 (Explotación de firmware) T1499 (Denegación de Servicio en Endpoint)	Compromiso de sensores de vigilancia, pérdida de información táctica o manipulación de datos.	Ataque Mirai Botnet (EE.UU., 2016)
Spoofing satelital	Suplantación de señales de posicionamiento y navegación satelital.	Deterioro del control de procesos / Evasión	T0856 (Mensaje de información falsa)	Afecta los sistemas de navegación, vigilancia aérea, control de tráfico aéreo y coordinación táctica.	Ataques registrados en Ucrania (2024)

Fuente: elaboración propia con base en la información obtenida de ENISA (2023 y 2024) y MITRE ATT&CK, (n.d.)

Como se observa en la tabla anterior, la variedad y sofisticación de las amenazas cibernéticas que enfrentan los CCOFA exige una visión integral y actualizada de los riesgos. No solo se trata de identificar a los actores y sus motivaciones, sino también de comprender

cómo pueden combinar diferentes técnicas y vectores de ataque para maximizar su impacto sobre infraestructuras críticas.

Dentro de esta perspectiva de amenazas avanzadas, cobra especial relevancia un nuevo vector emergente: los ataques dirigidos a sistemas de inteligencia artificial (IA). En el contexto actual, marcado por la rápida adopción de tecnologías inteligentes, se vuelve crucial considerar las amenazas derivadas de sistemas de inteligencia artificial (IA), especialmente en entornos militares donde estos sistemas se integran en decisiones críticas, armas autónomas, vigilancia y análisis predictivo.

Diversos organismos internacionales, como la OTAN y el MITRE, han desarrollado marcos específicos para clasificar y comprender estas amenazas. Destaca el marco ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems), una iniciativa conjunta que identifica tácticas, técnicas y procedimientos utilizados por adversarios para atacar, manipular o engañar sistemas de IA durante su entrenamiento, inferencia o funcionamiento en tiempo real (MITRE ATLAS, 2024).

La inclusión de estos riesgos resulta especialmente relevante para los CCOFA, ya que los sistemas C2 modernos incorporan cada vez más herramientas de IA para vigilancia, predicción de amenazas y toma de decisiones automatizada.

Este panorama global refuerza la importancia de contar con una inteligencia de ciberamenazas robusta y con marcos de referencia especializados que permitan identificar, de manera sistemática, las tácticas y técnicas empleadas por los atacantes, anticipando así sus movimientos.

Inteligencia de amenazas cibernéticas

En entornos militares como los CCOFA, la inteligencia de amenazas cibernéticas, por su

sigla en inglés CTI (Cyber-threat intelligence) es esencial para la toma de decisiones estratégicas. Ainslie et al. (2023) subrayan que la CTI proporciona un conocimiento detallado sobre amenazas y actores maliciosos, enriqueciendo el proceso decisorio en todos los niveles de la organización. Por ejemplo, una inteligencia de amenazas bien implementada permite a los altos mandos anticipar tácticas enemigas, lo que orienta tanto el diseño de estrategias defensivas como la asignación de recursos críticos.

Tanto Ainslie et al. (2023) como Yulianto et al. (2024) coinciden en que la CTI debe integrarse en un ciclo continuo de mejora, donde los resultados de ejercicios simulados y los informes de inteligencia alimenten la revisión constante de los sistemas defensivos. Esta retroalimentación es crucial en entornos como los CCOFA, donde la anticipación, la rapidez y la adaptación son claves para mantener la resiliencia cibernética.

Así, el fortalecimiento de la inteligencia de amenazas, se consolida como una estrategia imprescindible para anticipar, resistir y adaptarse frente a amenazas avanzadas. Esta perspectiva refuerza la toma de decisiones defensivas en entornos militares y sienta las bases para comprender cómo dichas amenazas pueden comprometer principios fundamentales de seguridad como la confidencialidad, integridad y disponibilidad.

A continuación, se presentan casos documentados que muestran cómo estas amenazas han comprometido sistemas militares y gubernamentales, permitiendo extraer lecciones clave para el fortalecimiento de los CCOFA.

Casos documentados de amenazas a sistemas militares y gubernamentales

En las últimas décadas, se han registrado ciberataques de gran impacto contra infraestructuras críticas gubernamentales y militares. Estos incidentes ofrecen información valiosa sobre las estrategias de los adversarios y el impacto potencial de las amenazas emergentes discutidas,

lo cual, no solo permiten entender el modus operandi de los adversarios, sino también identificar las debilidades explotadas y las consecuencias operacionales, aspectos esenciales para fortalecer la ciberresiliencia de los CCOFA.

- **Stuxnet (2010)**: Malware diseñado para sabotear el programa nuclear iraní, manipulando PLCs y demostrando cómo una ciberamenaza puede generar efectos físicos directos. Comprometió la integridad de los sistemas (Djenna et al., 2021, p. 6).
- **SolarWinds (2020)**: Ataque a la cadena de suministro realizado por APT29 (grupo ruso) que comprometió la plataforma Orion, afectando a más de 18.000 organizaciones, incluyendo agencias de defensa de EE. UU, comprometiendo la confidencialidad de la informacion (ENISA, 2023, p. 17).
- **NotPetya (2017)**: Ataque cibernético inicialmente disfrazado de ransomware, diseñado para causar destrucción. Propagado a través de actualizaciones de software contable en Ucrania, inutilizó sistemas y afectó la disponibilidad de compañías logísticas y entidades gubernamentales a nivel global (Flor-Unda et al., 2023, p. 14).

Como se ha evidenciado, el contexto actual de amenazas exige que los modelos defensivos evolucionen hacia enfoques más proactivos y adaptativos. En este sentido, el siguiente apartado abordará los marcos normativos y tecnológicos aplicables a la ciberresiliencia, proporcionando una base institucional y técnica que respalde la transformación resiliente de los CCOFA.

Marcos normativos y tecnológicos aplicables a la ciberresiliencia en los CCOFA

En entornos altamente críticos como los CCOFA, garantizar la ciberresiliencia implica adoptar marcos normativos y tecnológicos sólidos que permitan anticipar, resistir, recuperarse y adaptarse frente a amenazas cibernéticas complejas. Para lograrlo, la FAC recurre a estándares internacionales como las normas ISO, las guías del NIST de Estados Unidos y políticas públicas nacionales, como los documentos CONPES, que establecen lineamientos específicos para la seguridad digital en Colombia (Departamento Nacional de Planeación, 2011, p. 5; ISO&IEC, 2022, p. v; NIST CSF 2.0, 2024, p. 1).

Normas ISO claves para la ciberresiliencia

- ISO & IEC 27001:2022: Requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), abarcando la identificación de riesgos, evaluación de impactos y la aplicación de controles para proteger los principios de CIA de los activos críticos (ISO&IEC, 2022, pp. 1-10).
- ISO & IEC 22301:2019: Se centra en la gestión de la continuidad del negocio, estableciendo procedimientos para asegurar la operación de funciones esenciales ante situaciones de disrupción (ISO&IEC, 2019, pp. 12-19).
- ISO & IEC 27031:2025: Proporciona una guía específica para preparar la infraestructura TIC ante incidentes, fortaleciendo la capacidad de respuesta y recuperación (ISO&IEC, 2025, p. 1).

- ISO & IEC 27032:2023: Ofrece directrices para la ciberseguridad desde una perspectiva colaborativa, promoviendo la cooperación entre las partes interesadas (ISO&IEC, 2023, p. 3).

La integración de estas normas permite a los CCOFA gestionar los riesgos tecnológicos de manera sistémica y alineada con estándares internacionales.

Marcos y normas NIST aplicables

- NIST Cybersecurity Framework (CSF 2.0): Herramienta para diagnosticar y mejorar capacidades de seguridad, estructurada en funciones como Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. Además, es compatible con marcos como ISO 27001 y NIST SP 800-53, lo que permite articular políticas de defensa con controles específicos (NIST CSF 2.0, 2024, pp. 5-7).
- NIST SP 800-53 Rev. 5: Ofrece un catálogo de controles técnicos, físicos y administrativos, clasificados según impacto y criticidad. El proceso de adaptación (tailoring) permite seleccionar controles ajustados a las necesidades de los CCOFA, como los controles de planificación de contingencia (CP), protección de comunicaciones (SC), control de acceso (AC) y respuesta a incidentes (IR), fundamentales para la disponibilidad y seguridad de las funciones de mando y control (NIST SP 800-53 Rev. 5, 2020, pp. 1-12).
- NIST SP 800-160 Vol. 2: Introduce principios de ciberresiliencia y defensa en profundidad, alineados con arquitecturas como Zero Trust, que eliminan la confianza implícita y aplican autenticación continua y segmentación estricta de redes (Ross et al., 2021, pp. 18-22).

- NIST SP 800-34 Rev. 1: Guía que proporciona directrices detalladas para garantizar la continuidad operativa de los sistemas de información críticos mediante la planificación de contingencias específicas, que incluyan medidas preventivas y estrategias de recuperación adaptadas al nivel de impacto y a los requisitos de confidencialidad, integridad y disponibilidad del sistema. (Swanson et al., 2010, p. 1).

La integración de estos marcos y controles asegura coherencia entre la planificación estratégica y la implementación táctica en los CCOFA.

Normatividad y marcos en Colombia para los CCOFA

- CONPES 3701 (2011): Sentó las bases de la política pública en ciberseguridad y ciberdefensa, orientando la estrategia nacional para enfrentar amenazas cibernéticas y fortalecer capacidades estatales (Departamento Nacional de Planeación, 2011, p. 10).
- CONPES 3854 (2016): Actualizó el enfoque hacia una gestión integral del riesgo digital, promoviendo el uso de estándares internacionales y la articulación interinstitucional (Departamento Nacional de Planeación, 2016, p. 7).
- Política de Seguridad Digital del Estado: Impulsada por el MinTIC, se enfoca en la protección de infraestructuras críticas mediante el fortalecimiento de capacidades técnicas y humanas, exigiendo a los CCOFA integrar sus estrategias de ciberresiliencia con la normativa nacional vigente y los lineamientos de defensa nacional.

- Legislación penal y regulatoria: Incluye la actualización del Código Penal colombiano a través de la Ley 1273/2009, que tipifica los delitos informáticos y protege la información digital, así como el decreto 338/2022 que establecen medidas de protección de datos y obligan a operadores críticos a implementar controles técnicos alineados con estándares internacionales para garantizar la confidencialidad, integridad y disponibilidad de la información (Congreso de la República de Colombia, 2009, art. 2; Presidencia de la República de Colombia, 2022, art. 4).

Herramientas tecnológicas y mejores prácticas

La aplicación de estas directrices se potencia con herramientas tecnológicas avanzadas, como:

- SIEM (Security Information and Event Management) y EDR (Endpoint Detection and Response) para monitoreo en tiempo real, detección temprana de amenazas y análisis forense.
- Arquitectura Zero Trust, que elimina la confianza implícita y aplica autenticación continua y segmentación lógica (Ross et al., 2021, p. 70).
- SOAR (Security Orchestration, Automation and Response), que integra fuentes de información y ejecuta respuestas automáticas ante incidentes, reduciendo tiempos de reacción y minimizando impactos.

En conjunto, la adopción de normas internacionales, marcos regulatorios nacionales y herramientas tecnológicas específicas permite construir una arquitectura de ciberresiliencia robusta, adaptada al contexto estratégico y operativo de los CCOFA. Esta base normativa y

técnica sienta las condiciones para formular lineamientos operativos que fortalezcan la ciberresiliencia en los CCOFA, frente a las amenazas emergentes del entorno digital.

Propuesta de lineamientos de fortalecimiento de la ciberresiliencia en los CCOFA

Los hallazgos de esta investigación demuestran que la ciberresiliencia en los CCOFA debe abordarse como un esfuerzo integral que combine capacidades técnicas avanzadas con una estructura organizacional sólida. A partir de lo anterior se propone:

Fortalecer la gobernanza y cultura de ciberresiliencia

- Gobernanza y coordinación: Formar un comité de ciberseguridad con representantes del mando estratégico, operaciones y TI, asegurando su conexión con la política nacional y garantizando liderazgo con compromiso institucional.
- Cultura de resiliencia: Capacitar de manera continua al personal mediante campañas de concienciación y entrenamientos prácticos, con énfasis en las lecciones aprendidas de ejercicios recientes (Petrenko, 2019, p. 326), integrando estos procesos con mecanismos de liderazgo, comunicación interna y retroalimentación permanente, orientados a reducir resistencias organizacionales y fortalecer una cultura proactiva frente a la ciberresiliencia.

Gestión de la continuidad del servicio: BCP y DRP

Para garantizar la continuidad de las operaciones en los CCOFA, es fundamental contar con planes formales de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP). Estos planes deben detallar los pasos a seguir para restaurar servicios críticos después de un incidente grave, asegurando que las funciones esenciales sigan operativas mediante una

evaluación y mejora constante de los procedimientos de respuesta (Swanson et al., 2010, pp. 7-10).

- Desarrollo de DRP/BCP integrados: Incluir procedimientos de conmutación por error, replicación de datos y reasignación de funciones críticas, considerando el objetivo de tiempo de recuperación, por su sigla en inglés RTO (Recovery Time Objective) y el objetivo de punto de recuperación, por su sigla en inglés RPO (Recovery Point Objective), estén adecuados al impacto operativo, que en este caso sería de 5 a 15 minutos el RTO y de máximo 30 minutos el RPO (Petrenko, 2018, p. 291).
- Pruebas y actualización periódica: Realizar simulacros regulares que involucren tanto al equipo técnico como a las unidades de mando, validando la eficacia de los planes y aprendiendo de cada ejercicio. Se recomienda incorporar redundancias tecnológicas y verificar su funcionamiento en cada simulacro (Ross et al., 2021, p. 103; Petrenko, 2019, p. 308).
- Coordinación con gestión de incidentes: Integrar los planes de continuidad con los procedimientos de gestión de incidentes, asegurando una respuesta coordinada y eficiente (CISA, 2020, p. 10; Petrenko, 2019, p. 335).

Arquitectura resiliente para la infraestructura crítica

La infraestructura de los CCOFA debe diseñarse bajo principios de resiliencia, aplicando redundancia y segmentación. Esto significa contar con múltiples instancias protegidas de cada recurso crítico, de modo que, si un componente falla, otro pueda asumir su función sin afectar la operación (Ross et al., 2021, pp. 103-104).

- Sistemas redundantes: Desplegar hardware en alta disponibilidad y sitios geo-replicados para los centros de datos, garantizando una recuperación rápida ante interrupciones físicas. Es importante complementar los respaldos tradicionales con otras defensas avanzadas (Ross et al., 2021, p. 103). Para esto se debe tener inventarios de componentes de hardware con un sistema de predicción de fallos, basado en los tiempos de vida útil dados por los fabricantes o eventos reales ocurridos.
- Defensa en profundidad coordinada: Implementar varias capas de protección (firewalls, IDS/IPS, autenticación robusta, cifrado de extremo a extremo) que trabajen de manera conjunta para contener cualquier intento de intrusión (Ross et al., 2021, p. 95).
- Segmentación física y lógica: Separar físicamente las instalaciones sensibles y las redes de control de misión de las redes administrativas, utilizando VLANs y zonas desmilitarizadas (DMZ) para dividir el acceso y asegurar que cada segmento crítico cuente con su propio monitoreo y capacidad de recuperación (Ross et al., 2021, pp. 103-104).

Simulaciones de ciberincidentes y entrenamiento Red Team/Blue Team

Para poner a prueba la resiliencia de la defensa, es esencial establecer un programa continuo de ejercicios tácticos a través del laboratorio INSIDE de la DICAE. Los equipos Red Team (DICAE) simulan ataques reales, mientras que los Blue Team (DISIE) se encargan de responder y mitigar los incidentes, utilizando tácticas basadas en marcos reconocidos como MITRE ATT&CK (Yulianto et al., 2025, p. 9). Adicional, se debe adoptar un enfoque colaborativo en ciberseguridad que integra y coordina las funciones de ambos equipos a

través del Purple Team, cuyo objetivo es fortalecer de manera constante las defensas de la organización mediante el aprendizaje mutuo (Dale, 2020, p. 1).

- Ejercicios periódicos de Hacking ético: Planificar ejercicios anuales de penetración controlada y escenarios de ataque avanzados, con el objetivo de validar la efectividad de los controles en tiempo real (Yulianto et al., 2025, p. 2).
- Integración de inteligencia de amenazas: Utilizar los resultados de los ejercicios como retroalimentación para mejorar continuamente las reglas de detección y los planes de respuesta (Yulianto et al., 2025, p. 8).
- Capacitación y lecciones aprendidas: Realizar sesiones de formación después de cada ejercicio y actualizar políticas y procedimientos en función de las lecciones aprendidas (Yulianto et al., 2025, p. 9), generando un sistema de gestión de conocimiento postmortem.

Por último, se propone complementar los mecanismos tradicionales de continuidad con prácticas avanzadas de resiliencia tecnológica. Entre estas, se recomienda la incorporación de principios de Chaos Engineering, que consisten en realizar pruebas controladas para simular fallas reales en los sistemas, con el fin de evaluar las respuestas del equipo, la eficacia de los procedimientos y la tolerancia real de la infraestructura (Rosenthal & Jones, 2020, p. 237).

En este marco, es clave institucionalizar ejercicios tipo "Game Day", en los que los equipos de Ciber a traves de la DICAE y de Tecnologias de la Informacion y Comunicación a traves de la DISIE, participen activamente en la detección, análisis y resolución de incidentes simulados (Rosenthal & Jones, 2020, p. 256). Estos ejercicios no solo permiten

validar la preparación técnica, sino también la comunicación, la toma de decisiones bajo presión y la coordinación interfuncional.

Priorización según impacto operacional

No todos los activos y servicios tienen la misma importancia para la misión. Por eso, se recomienda realizar un análisis de impacto al negocio, por su sigla en inglés BIA (Business Impact Analysis), permitiendo clasificar los componentes clave, identificando las "joyas de la corona" y asignándoles la máxima protección (Ross et al., 2021, pp. 113-114; Petrenko, 2019, p. 287).

- Clasificación de activos: Determinar la criticidad de cada servicio según el daño operativo que causaría su interrupción (Petrenko, 2019, p. 297).
- Priorización de defensas y recursos: Asignar mayor presupuesto y esfuerzos a los activos de mayor impacto, como los sistemas radar prioritarios (Petrenko, 2018, p. 278).
- Revisión dinámica: Actualizar la priorización de activos y defensas de forma anual o cuando cambien las condiciones operativas, para que siempre reflejen el impacto real en la misión.

Medición de la resiliencia: KPIs e indicadores de madurez

Para saber si las estrategias de ciberresiliencia están funcionando, es fundamental definir indicadores clave (KPIs) y métricas de madurez. El modelo CRR recomienda medir la resiliencia operativa tanto en tiempos normales como en situaciones adversas (CISA, 2020, pp. 16-17; Petrenko, 2018, p. 189).

- Indicadores cuantitativos: Medir mensualmente métricas operacionales y de seguridad, registrando los KPIs en cuadros de mando para identificar tendencias y áreas de mejora (Petrenko, 2019, p. 189).
- Niveles de madurez: Utilizar los Niveles Indicadores de Madurez (MIL) del CRR para evaluar las capacidades en cada dominio (CISA, 2020, pp. 16-17; Petrenko, 2019, p. 353).
- Informes periódicos: Elaborar reportes que integren KPIs y niveles MIL, guiando la toma de decisiones y el perfeccionamiento de la estrategia (Petrenko, 2019, p. 326).

Esta propuesta, basada en seis lineamientos organizativos, técnicos y estratégicos, constituye un marco integral alineado con el NIST SP 800-160 Vol.2, el modelo CRR y la literatura académica sobre ciberresiliencia. La validez y el rigor académico de la propuesta fueron confirmados mediante el método DELPHI, con la aprobación de tres expertos.

Por lo tanto, la adopción de estos criterios permitirá que los CCOFA anticipen, resistan, se recuperen y se adapten ante ciberamenazas, garantizando la continuidad de la misión y fortaleciendo la soberanía digital y operativa de la Fuerza Aeroespacial Colombiana.

Conclusiones

El estudio permitió obtener una visión clara sobre el estado de la ciberresiliencia en los CCOFA. Se identificaron fortalezas notables en la madurez organizacional y técnica, especialmente en la gestión de activos y la aplicación de controles, en línea con los marcos internacionales y nacionales vigentes.

Un aspecto relevante es que los CCOFA funcionan como sistemas complejos adaptativos (CAS), donde la interacción dinámica entre personas, tecnología y

procedimientos genera capacidades emergentes para adaptarse a entornos cambiantes y enfrentar amenazas inesperadas. Sin embargo, también se detectaron brechas importantes en la gestión de la continuidad del servicio, especialmente en la formalización y validación de los planes de recuperación ante desastres y continuidad del negocio.

El análisis de amenazas emergentes, como los ataques persistentes avanzados, el ransomware y el sabotaje cibernético, puso de manifiesto la necesidad de fortalecer la inteligencia de amenazas y de integrar marcos como MITRE ATT&CK para mejorar la capacidad de detección y respuesta. La propuesta desarrollada se articuló con los lineamientos del NIST SP 800-160 Vol. 2 y el modelo CRR, lo que permitió consolidar un enfoque sistémico y metodológicamente robusto para el diseño y la evaluación de sistemas ciberresilientes en entornos críticos.

El principal aporte del trabajo fue la formulación de lineamientos estratégicos y técnicos que integran gobernanza, cultura organizacional, arquitectura resiliente, continuidad del servicio, ejercicios tácticos, priorización y métricas de madurez, todo ello orientado a fortalecer la ciberresiliencia en entornos militares críticos. Este enfoque adaptativo contribuye directamente a la sostenibilidad operativa y a la protección de la soberanía digital.

Cabe señalar que una limitación relevante del estudio fue la dependencia de información sensible, lo que restringió al principio el acceso a expertos de la FAC y la búsqueda de literatura especializada sobre el tema.

Finalmente, se sugiere avanzar en la implementación progresiva de los lineamientos propuestos, reforzar la capacitación continua y fomentar la colaboración interinstitucional, con el fin de mantener una postura resiliente ante amenazas cibernéticas en constante evolución.

Referencias

Acur, S., & Hendriks, T. (2024). *The Need for Cyber-Resilience in Complex Systems*. 2024 IEEE International Conference on Cyber Security and Resilience (CSR), 480–485. https://doi.org/10.1109/CSR61664.2024.10679396

Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. Applied Sciences, 14(24), 11807. https://doi.org/10.3390/app142411807

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers & Security, 132, 103352. https://doi.org/10.1016/j.cose.2023.103352

Araujo, M. S. d., Machado, B. A. S., & Passos, F. U. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. Applied Sciences*, 14*(5), 2116. https://doi.org/10.3390/app14052116

Baesystems.com. (n.d.). *C4ISR Systems*. Retrieved June 19, 2025, from https://www.baesystems.com/en-us/who-we-are/electronic-systems/c4isr

Bagrodia, R. (2023). Using network digital twins to improve cyber resilience of missions. Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 20*(1), 97–106. https://doi.org/10.1177/15485129221131226

Bodeau, D., Graubart, R., Picciotto, J., & McQuaid, R. (2011, September 1). Cyber resiliency engineering framework. MITRE. https://www.mitre.org/news-insights/publication/cyber-resiliency-engineering-framework

Carmichael, T., & Hadzikadic, M. (2019). The fundamentals of complex adaptive systems. In M. Hadzikadic, S. O'Brien, & M. Khouja (Eds.), *Managing complexity: Practical* considerations in the development and application of agent-based models (pp. 3–21). Springer. https://doi.org/10.1007/978-3-030-20309-2_1

CISA. (2020). *Cyber Resilience Review (CRR): Method description and self-assessment user guide*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/2_CRR%25204.0_Self-Assessment_User_Guide_April_2020.pdf

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre*

otras disposiciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34492

Conklin, W. A., & Shoemaker, D. (2017). *Cyber-resilience: Seven steps for institutional survival*. EDPACS, 55(2), 14–22. https://doi.org/10.1080/07366981.2017.1289026

Consejo de la Unión Europea. (2008). *Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección*. Diario Oficial de la Unión Europea, L 345, 75–82. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008L0114

Cyber resiliency level®. (n.d.). Lockheed Martin. Retrieved April 24, 2025, from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-resiliency-level.html

Cybersecurity and Infrastructure Security Agency. (2020, April). *Cyber Resilience Review (CRR): Method description and self-assessment user guide*. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/2_CRR%25204.0_Self-Assessment_User_Guide_April_2020.pdf

Dale, C. (2020). *Red, blue and purple teams: Combining your security capabilities for the best outcome*. SANS Institute. https://www.sans.org/media/analyst-program/red-blue-purple-teams-combining-security-capabilities-outcome-39190.pdf

de Nobrega, K. M., Rutkowski, A.-F., & Saunders, C. (2024). *The whole of cyber defense: Syncing practice and theory.* The Journal of Strategic Information Systems, *33*(4), 101861. https://doi.org/10.1016/j.jsis.2024.101861

Departamento Nacional de Planeación. (2011). *Lineamientos de política para ciberseguridad y ciberdefensa (Documento CONPES 3701)*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación. (2016). *Política nacional de seguridad digital (Documento CONPES 3854)*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Díaz Mardones, J. (2021). *Infraestructuras críticas y ciberseguridad: una aproximación desde América Latina*. Revista de Derecho Público, (175), 63–84. https://publicacionesacague.cl/index.php/tica/article/view/175/198

Djenna, A., Harous, S., & Saidouni, D. E. (2021). *Internet of Things meet Internet of Threats: New concern cyber security issues of critical cyber infrastructure*. Applied Sciences, 11(10), 4580. https://doi.org/10.3390/app11104580

European Commission. (2022). *Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*. https://ec.europa.eu/newsroom/ECCC/items/757902/en

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. (2023). *A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America. Informatics*, 10(3), 71. https://doi.org/10.3390/informatics10030071

Fuerza Aérea Colombiana. (2013). *Manual de doctrina básica aérea y espacial (MADBA) (4ª ed.)*. Comando Fuerza Aérea Colombiana.

Fuerza Aérea Colombiana. (2019). *Cartilla de políticas institucionales* (Versión del 27 de enero de 2019) [Documento institucional no publicado].

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. P. (2014). *Metodología de la investigación (6.ª ed.)*. McGraw-Hill Interamericana.

Holland, J. H. (1992). *Complex adaptive systems*. *Daedalus, 121*(1), 17–30. https://www.jstor.org/stable/20025416

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022*: *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (3.ª ed.). https://www.iso.org/standard/27001

International Organization for Standardization & International Electrotechnical Commission. (2019). *ISO/IEC 27001:2022*: *Security and resilience — Business continuity management systems — Requirements* (2.ª ed.). https://www.iso.org/standard/75106.html

International Organization for Standardization & International Electrotechnical Commission. (2019). *ISO/IEC 27031:2025*: Cybersecurity — Information and communication technology readiness for business continuity (2.ª ed.). https://www.iso.org/standard/27031

International Organization for Standardization & International Electrotechnical Commission. (2023). *ISO/IEC 27032:2023*: Cybersecurity — Guidelines for Internet security(2.ª ed.). https://www.iso.org/standard/76070.html

MITRE ATLAS. (2024). *Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS)*. https://atlas.mitre.org

MITRE ATT&CK. (n.d.). Mitre.org. Retrieved July 6, 2025, from https://attack.mitre.org/

National Cyber Security Centre. (2024). *Cyber Assessment Framework (CAF)*. https://www.ncsc.gov.uk/collection/cyber-assessment-framework

Petrenko, S. (2019). *Cyber resilience*. River Publishers. https://doi.org/10.1201/9781003337300

Poulter, A.J.; Cox, S.J. *Enabling Secure Guest Access for Command-and-Control of Internet of Things Devices*. *IoT* 2021, *2*, 236-248. https://doi.org/10.3390/iot2020013

Presidencia de la República de Colombia. (2022). *Decreto 338 de 2022: Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=181866

Rosenthal, C., & Jones, N. (2020). *Chaos engineering: System resiliency in practice*. O'Reilly Media, Inc.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach (NIST Special Publication 800-160, Volume 2, Revision 1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

Swanson, M., Bowen, P., Wohl Phillips, A., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems (NIST Special Publication 800-34 Rev. 1)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

The White House. (2013). *Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21)*. https://www.cisa.gov/sites/default/files/publications/ppd-21-critical-infrastructure-security-and-resilience-508.pdf

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. International Journal of Information Security, 23, 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

World Economic Forum. (2022). *Cyber Resilience Index: Advancing cyber resilience across sectors and regions*. https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf

Yulianto, S., Soewito, B., Gaol, F. L., & Kurniawan, A. (2025). Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration: A paradigm shift in cybersecurity assessment. Cyber Security and Applications, 3, 100077. https://doi.org/10.1016/j.csa.2024.100077