ARTÍCULO DOI 10.52781/cmm.a202

Una nueva perspectiva para la Red Operativa de Defensa (ROD): Integración a nivel de Personas, Procesos y Tecnologías

A new vision for the Defense Operational Network (DON): Integration at the Levels of People, Processes, and Technologies

Resumen: El panorama mundial actual, caracterizado por una fuerte interdependencia entre los países y por rápidas transformaciones políticas, económicas y tecnológicas, ha acentuado la inestabilidad en diversas regiones. Las disputas comerciales, informáticas y cibernéticas ocurren constantemente, y las Fuerzas de Defensa Internacionales están replanteándose sus estrategias: o bien intensifican su cooperación para superar los desafíos comunes, o bien adoptan una reestructuración profunda, adaptándose a las exigencias del presente. La doctrina brasileña prevé integraciones periódicas en operaciones conjuntas, mientras que, a diario, cada Fuerza Individual tiene sus propios objetivos, planes y acciones, y coordina de manera autónoma y a nivel interno su infraestructura de Tecnología de la Información y de las Comunicaciones. Este artículo propone una nueva visión para la Red Operativa de Defensa (ROD), capaz de reunir capacidades conjuntas e integrar de manera continua a las personas, los procesos y las tecnologías. En este contexto tan dinámico, costoso y con escasez de inversiones, la unión de esfuerzos en la planificación y la construcción de una infraestructura única y flexible puede acelerar el desarrollo y la capacidad de defensa nacional.

Palabras clave: Ciencias Militares; Defensa; Integración; Red Operativa de Defensa; SD-WAN.

Abstract: The current global scenario, marked by strong interdependence between countries and rapid political, economic, and technological transformations, has exacerbated instability in several regions. Trade, information, and cyber disputes are constantly occurring, and the International Defense Forces are rethinking their strategies: either intensifying cooperation to overcome common challenges or adopting a profound restructuring to adapt to current demands. Brazilian doctrine provides for periodic integrations in joint operations, while each Singular Force has its own daily objectives, plans, and actions, which coordinate their Information and Communications Technology infrastructure internally. This article proposes a new vision for the Defense Operational Network, capable of aggregating joint capabilities and continuously integrating people, processes, and technologies. In such a dynamic, costly, and underinvested environment, joint efforts in planning and building a single, flexible infrastructure can accelerate the development and power of national defense.

Keywords: Military Science; Defense; Defense Operational Network; Integration; SD-WAN.

Igor David Brito Caldeira
Exército Brasileiro. Instituto Militar de Engenharia (IME). Programa de Pós-Graduação em Engenharia de Defesa (PGED).
Rio de Janeiro, RJ, Brasil.
caldeira.igor@ime.eb.br

Ronaldo Moreira Salles
Exército Brasileiro. Instituto Militar de Engenharia (IME). Programa de Pós-Graduação em Engenharia de Defesa (PGED).
Rio de Janeiro, RJ, Brasil.
salles@ime.eb.br

Recibido: 30 jul. 2025
Aceptado: 09 abr. 2026

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 INTRODUCCIÓN

En la historia militar mundial, las acciones integradas entre las Fuerzas Armadas (FFAA) son comunes. Sin embargo, la gran y rápida evolución tecnológica, acelerada y potenciada por el desarrollo de la Inteligencia Artificial (IA), ha impulsado la reformulación de conceptos y doctrinas que influyen en el arte de la guerra en la actualidad.

A principios de la década de 2020, los líderes estadounidenses tomaron medidas para ampliar y desarrollar sistemas conjuntos en Estados Unidos, señalando la necesidad de mejorar los sistemas e integrar las capacidades conjuntas (Estados Unidos da América, 2021). Más concretamente, se desarrolló una estrategia específica para la integración completa del Comando y Control (C^2) Conjunto e Integrado, denominada "*Joint All-Domain Command and Control (JADC2) Strategy*" (Estados Unidos da América, 2022).

Otros países se han dado cuenta de los cambios en el modelo de los recientes conflictos globales, como los observados en la guerra entre Rusia y Ucrania, en la que los atacados desarrollaron rápidamente las "*Unmanned Systems Forces*", una nueva fuerza armada no tripulada con capacidad para actuar por tierra, mar y aire en la primera línea de combate, con un alcance de más de 2.000 km (Ucrânia, 2025). En consonancia con esto y de manera aún más amplia, el Reino Unido dio a conocer recientemente una política integrada que coordina su transición de una operación conjunta a una integrada en los próximos diez años, apuntando incluso a la creación de una nueva Fuerza Integrada (Reino Unido, 2025), encargada de mantener la base digital común y de gestionar los datos compartidos, tan esenciales para el nuevo modelo de guerra definida por software.

A pesar de los avances en materia de doctrina, la Red Operativa de Defensa (ROD) de Brasil aún enfrenta el reto de la fragmentación, ya que opera como un conjunto de sistemas independientes (Recim, EBNet e Intraer) con administraciones aisladas. La brecha identificada radica en la falta de un modelo que integre estas infraestructuras, no solo desde el punto de vista tecnológico, sino también de manera coordinada con las personas y los procesos organizativos. Ante esto, este artículo responde a la siguiente pregunta de investigación: ¿cómo hacer viable una infraestructura de conectividad única y flexible que cumpla con los requisitos de soberanía e interoperabilidad de las Fuerzas Armadas? El objetivo de este trabajo es proponer una nueva visión para la ROD, basada en la tecnología *Software-Defined Wide Area Network* (SD-WAN), que funcione como un sistema de sistemas integrado bajo una gobernanza compartida.

La principal aportación de este manuscrito es la propuesta de un modelo organizativo y conceptual para la integración de la ROD. Este estudio no se limita al diagnóstico, sino que plantea una arquitectura de red de larga distancia definida por software (SD-WAN) como el motor para la evolución de la base digital común de la Defensa. En este sentido, el mundo avanza hacia el fomento de una evolución doctrinal que promueva la aproximación entre las FFAA y consolide la infraestructura de operaciones conjuntas, desde su planificación hasta el cumplimiento de la misión final. A continuación, se presentará una nueva visión para la ROD, con el objetivo de lograr una mayor integración de la infraestructura de conectividad y de datos a nivel de personas, procesos y tecnologías, en consonancia con el aumento del intercambio de mano de obra, conocimientos e inversiones. De esta manera, será posible lograr una integración informativa completa, así como una mayor seguridad cibernética, aprovechando el potencial de la IA para resolver y hacer frente a las vulnerabilidades y amenazas, lo que también permitirá demostrar el avance en el logro de los objetivos nacionales permanentes.

2 REVISIÓN TEÓRICA, DESARROLLO Y METODOLOGÍA

A finales de la última década, Brasil actualizó y estableció nuevos procedimientos para orientar las operaciones conjuntas en el país. La Doctrina para el Sistema Militar de Comando y Control (SisMC²) establece los principios básicos de C² en su planificación y ejecución: unidad de comando, simplicidad, seguridad, flexibilidad, confiabilidad, continuidad, rapidez, amplitud e integración (Brasil, 2015). La Doctrina de Operaciones Conjuntas establece que las planificaciones conjuntas deben basarse en los principios de universalidad, unidad, objetividad, flexibilidad, coordinación e interoperabilidad (Brasil, 2020). Se puede observar que solo "unidad" y "flexibilidad" son elementos comunes en las exigencias de ambas doctrinas.

Recientemente se aprobó la actualización de la Estrategia Nacional de Defensa (END), en la que se reafirma que el estado de alerta deseado es el resultado de la evolución continua en el proceso de transformación y de la búsqueda de nuevas capacidades, guiadas por características doctrinales de flexibilidad, adaptabilidad, modularidad, elasticidad y sostenibilidad (Brasil, 2025a). En consecuencia, se elaboró el Plan Estratégico Sectorial de Defensa (PESD) para los próximos 12 años (2024-2035), con el objetivo de proporcionar directrices para obtener nuevas capacidades que respondan a los desafíos de la defensa con la rapidez y la eficacia necesarias, con miras a alcanzar el grado de madurez requerido para lograr el salto estratégico deseado (Brasil, 2025b). Al comparar esta evolución con las demandas anteriores, se destaca que la flexibilidad es el único factor común en todas ellas.

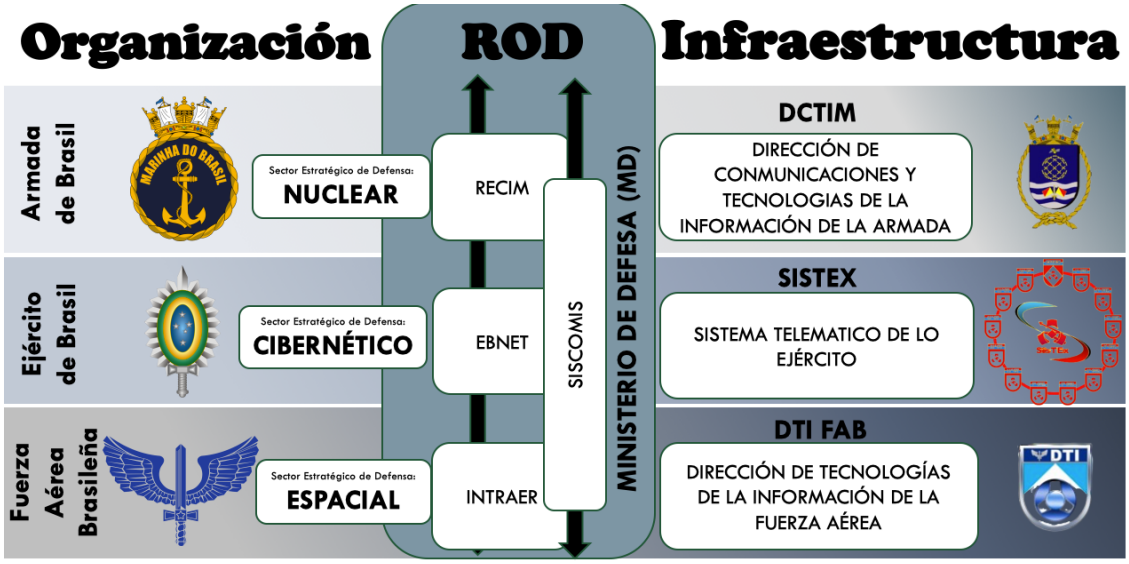
El Concepto Operativo del Sistema de Información de Apoyo a la Toma de Decisiones para el Comando y Control (SIADC²) enumera los principales Sistemas de Información/Sistemas de Apoyo a la Toma de Decisiones (SI/SAD) del Estado Mayor Conjunto de las Fuerzas Armadas (EMCFA) y de las FFAA, organizándolos en una estructura de Sistema de Sistemas (SdS). Es decir, se trata de un conjunto o una combinación de sistemas independientes, reunidos para proporcionar una capacidad que no es posible obtener con cada uno de esos sistemas por separado (Brasil, 2019). Sin embargo, la integración de una serie de sistemas independientes no equivale a un sistema único, en el que cada dato se comparte y se estructura de manera lógica, y toda su información es conocida por una inteligencia lógica central.

De este modo, ante escenarios mundiales dinámicos, la flexibilidad doctrinal es proporcionalmente mayor cuanto mayor es la flexibilidad de su infraestructura, lo que permite desarrollar la capacidad de reflejar rápidamente los cambios en los niveles estratégico, operativo y táctico. En la búsqueda de una mayor visibilidad y sinergia entre redes y sistemas, es recomendable plantearse el proceso para ampliar el uso compartido de una única red e infraestructura de datos para todas las FFAA, con el objetivo de desarrollar y sumar capacidades conjuntas.

2.1 Desarrollo

La ROD es la red que integra y presta servicios al SisMC² (BRASIL, 2023a), y está compuesta por un conjunto de enlaces de comunicación de datos militares operativos del tipo *Wide Area Network* (WAN). Consiste en la infraestructura por la que transitan los datos y la información de defensa, y cuenta con conexiones segregadas y diversificadas en los segmentos espacial y terrestre. También incluye las redes de datos de las FFAA (Recim, EBNet e Intraer) y, en casos específicos, el acceso seguro a Internet (Brasil, 2019), tal como se muestra en la Figura 1.

Figura 1 – Organización y estructura de la ROD actual



Fuente: Elaborado por el autor.

Recim es la Red de Comunicaciones Integradas de la Armada, que conecta a sus diversas Organizaciones Militares (OM) y extiende su alcance a los buques en misión en el extranjero y a la Estación Antártica Comandante Ferraz (EACF). De esta manera, facilita el intercambio de información entre los nueve distritos navales, encargados de coordinar y controlar las operaciones en sus respectivas áreas de jurisdicción, consolidándose así como un elemento fundamental para la eficacia de las comunicaciones navales (Marinha do Brasil, 2025). Por lo tanto, corresponde al Departamento de Comunicaciones y Tecnología de la Información de la Armada (DCTIM):

> [...] Garantizar la eficiencia y la eficacia del Sistema de Comunicaciones de la Armada (SISCOM) y de las actividades de prevención y protección del Espacio Cibernético de interés para la Armada (ECiber-MB), con el fin de contribuir a la preparación y el empleo del Poder Naval, del Sistema Naval de Guerra Cibernética (SisNavGCiber) y del Sistema Militar de Defensa Cibernética (SMDC). [...] proporcionar servicios flexibles, integrados e interoperables de Tecnología de la Información y las Comunicaciones (TIC), con confiabilidad, seguridad y rapidez (Marinha do Brasil, 2025, p. 2).

EBNet es la Red de Datos Corporativa del Ejército, que funciona como una intranet corporativa y privada, cuyo objetivo es interconectar las redes metropolitanas y locales del Ejército Brasileño (EB) para la transmisión de datos, voz e imágenes entre las OM (Exército Brasileiro, 2013). El Sistema de Telemática del Ejército (SisTEx) se encarga de proporcionar la infraestructura de conectividad (TIC) para los demás sistemas y medios que forman parte del Sistema de Comando y Control (SC^2Ex), bajo la dirección del Centro Integrado de Telemática del Ejército (CITEx) (Exército Brasileiro, 2024a, p. 2). Además, el SisTEx cuenta con 12 Centros de Telemática,

que son unidades operativas distribuidas geográficamente por todo Brasil y que prestan apoyo a las OM en todo el territorio nacional.

Por su parte, Intraer es la red interna del Comando de la Aeronáutica (Comaer), encargada de proporcionar las comunicaciones internas y el acceso a los sistemas de la Fuerza Aérea Brasileña (FAB). La División de Tecnología de la Información (DTI) de la Fuerza Aérea se encarga del desarrollo y el soporte de los sistemas corporativos, los simuladores de vuelo y la seguridad de la información, y desempeña funciones administrativas y operativas, además de llevar a cabo actividades de capacitación y gestión de recursos humanos en todas sus áreas de responsabilidad (Força Aérea Brasileira, 2023).

Para redundancia entre los niveles de comando más altos, existe una integración complementaria de telefonía y datos compuesta por sistemas satelitales, lo que permite una mayor coordinación y cooperación entre las tres FFAA brasileñas (Neto, 2023). El Sistema de Comunicaciones Militares por Satélite (Siscomis) es capaz de garantizar la continuidad de las comunicaciones críticas, incluso en situaciones en las que las redes comerciales no funcionan, y asegurar la continuidad del C^2.

2.2 Metodología

Esta investigación es de carácter cualitativo y exploratorio. El procedimiento metodológico consistió en una revisión bibliográfica y un análisis documental de las directrices estratégicas y las doctrinas militares nacionales e internacionales (Estados Unidos, Reino Unido y Ucrania). Además, se realizó un análisis reflexivo sobre la experiencia institucional en la implementación de la tecnología SD-WAN en entornos de crisis, específicamente durante la Operación Taquari II en Río Grande del Sur, con el fin de validar las premisas del modelo propuesto.

En el ámbito del Ministerio de Defensa (MD), se observa que cada una de las Fuerzas Armadas cuenta con una infraestructura de TIC gestionada de manera autónoma e independiente, alineada con las directrices de la Alta Jerarquía e integrada en puntos estratégicos. Sin embargo, este estudio busca presentar la oportunidad de integrar las redes corporativas desde su planificación hasta su implementación, desarrollando una infraestructura de red única, totalmente integrada, con gestión compartida y capaz de cumplir con todos los requisitos normativos.

Según la END (Brasil, 2025a), el sector estratégico más relacionado con el tema de la conectividad es el cibernético, que está liderado por el EB, pero que también cuenta con la participación de la Armada de Brasil (MB) y la FAB en la capacitación, la protección, la respuesta y la coordinación de sus actividades de respuesta ante incidentes en la red interna (Força Aérea Brasileira, 2025). Dichos esfuerzos se realizan también en colaboración con el Comando de Defensa Cibernética (ComDCiber), cuya misión es planificar, orientar, coordinar y controlar las actividades operativas, doctrinales, de desarrollo y de capacitación en el marco del Sistema Militar de Defensa Cibernética (SMDC) (Brasil, 2017), el cual asumió el papel de órgano central con el objetivo de garantizar el uso efectivo del espacio cibernético por parte de las Fuerzas Armadas e impedir o dificultar su utilización en contra de los intereses de la Defensa Nacional. Sin embargo, al CITEx le corresponde la misión de implementar y mantener el SC^2Ex, integrado al Sistema de Comando y Control de la Fuerza Terrestre (SC^2FTer), con el fin de permitir el flujo seguro y oportuno de información a los comandantes en todos los niveles, contribuyendo así al aumento del poder de combate del Ejército y al desarrollo nacional (Exército Brasileiro, 2024b).

En los ámbitos personal, procesal y tecnológico, la Doctrina Operativa del Ejército exige que su SC²Ex sufra el mínimo de cambios en sus bases físicas y lógicas, y que se adapte rápidamente a los cambios de la situación, empleando múltiples posibilidades de conexión y flexibilidad, lo que garantiza la continuidad, la confiabilidad y la seguridad (Exército Brasileiro, 2021). El EB reguló la organización y el funcionamiento del SC²Ex, estableciendo premisas, directrices y atribuciones:

> "En el contexto de las operaciones de convergencia, el C² es indispensable para garantizar la interoperabilidad conjunta, combinada e interinstitucional, lo que contribuye a la actuación del Ejército en todos los dominios (terrestre, marítimo, aéreo, cibernético, electromagnético y espacial) y en todas las dimensiones del combate (física, humana e informacional)" (Exército Brasileiro, 2024a, p. 2).

La gobernanza del SEC²Ex está a cargo del Estado Mayor del Ejército (EME) y la gestión de estos sistemas la lleva a cabo el Departamento de Ciencia y Tecnología (DCT). De esta manera, se da una colaboración integrada y coordinada dentro del EB, siendo responsabilidad del CITEx gestionar los proyectos y el funcionamiento de la infraestructura de EBNet. Dicho esto, podría ser interesante aumentar la sinergia y la integración entre las redes de todas las FFAA, y el camino más lógico para lograr una mayor cobertura y distribución en todo el territorio nacional recaería en el SisTEx. En ese mismo sentido, se facilitaría el acceso de la MB y la FAB a los *data centers* del Ejército, integrando de manera complementaria los datos y la información y proporcionando: una mejor gestión interinstitucional del personal, con la ampliación de la capacidad de gestión operativa de la red y de respuesta ante incidentes, además de la optimización de los recursos en la capacitación y la difusión del conocimiento; una mejor gestión de los procesos, mediante el intercambio de recursos en inversiones centralizadas, la consolidación de las mejores prácticas y la unificación de los marcos normativos; y una mejor gestión tecnológica, mediante la aplicación de recursos combinados en los controles de las políticas y en las operaciones de red totalmente integradas en materia de conectividad y alojamiento de sitios web y sistemas críticos, lo que contribuye a los servicios de inteligencia, las operaciones conjuntas y el desarrollo tecnológico integrado.

3 DESAFÍOS DE INVESTIGACIÓN IDENTIFICADOS

Como consecuencia de la Política de Defensa Cibernética, la Secretaría de Defensa creó el SMDC y estableció lo siguiente:

> "La capacidad de interacción interinstitucional del órgano central del SMDC se caracteriza por la colaboración con representantes de organismos de la administración pública federal, de infraestructuras críticas y de otros organismos, instituciones y empresas, tanto públicas como privadas, de interés para la Defensa" (Ministério da Defesa, 2020, p. 1).

En este contexto, es común que, en el ámbito personal, la coordinación del Ministerio de Defensa y de su EMCFA se relacione con los Estados Mayores de las Fuerzas Singulares. En cuanto a los procesos, la obtención y la aplicación de la capacidad de defensa cibernética, así como el manejo de incidentes de redes, siguen siendo responsabilidad independiente de la MB, el EB y

la FAB, con autonomía para planificar, implementar y controlar su infraestructura y su modo de operación, además de la elaboración y supervisión de las normas internas.

Los desafíos en el ámbito tecnológico se rigen por una cuestión paradójica, según la Doctrina Militar de Defensa Cibernética:

> "Paradoja tecnológica: cuanto mayor es el desarrollo tecnológico, mayor es la dependencia de la TI y, en consecuencia, mayor es la vulnerabilidad ante los ataques cibernéticos. Sin embargo, paradójicamente, las condiciones de defensa frente a los ataques cibernéticos son mejores gracias al alto grado de desarrollo tecnológico" (Brasil, 2023b, p. 22).

Sin embargo, la IA se ha convertido en un factor clave en los conflictos militares actuales, ya que es capaz de obtener datos de diversas fuentes, procesar un volumen inmenso de información y analizar situaciones a gran velocidad para la toma de decisiones de las Fuerzas Armadas (Pederneiras, 2024). De este modo, ante el creciente uso de la IA en el control de la automatización robótica que se observa a nivel mundial, resulta esencial buscar el desarrollo y la independencia en el sector tecnológico de la defensa.

Los retos de gobernanza y gestión de la EBNet están vinculados al binomio "necesidad versus posibilidad" (Santos; Oliveira; Belderrain, 2022). La migración de servicios a la nube digital aumenta la demanda de ancho de banda en la conectividad entre las OM y los *data centers*. La rentabilidad que ofrece la concentración de inversiones en data centers está relacionada con la necesidad de recursos para satisfacer el aumento de la demanda de capacidad y el dimensionamiento de cada enlace de EBNet, lo que choca con las diferencias de perspectivas e intereses de los distintos *stakeholders*.

Una gran dificultad tecnológica que se ha puesto de manifiesto es el reto que representa la estandarización de los equipos utilizados. Desde los inicios de las comunicaciones por radio analógicas hasta los modelos recientes de complejas redes digitales, las comunicaciones siguen vinculadas a diferentes tecnologías propietarias y, por ello, presentan limitaciones de integración entre distintos fabricantes. Es propio de la industria utilizar estándares propios y cerrados para imponer el uso de sus familias de productos en toda la organización. Los problemas derivados de la falta de estandarización son más evidentes en el comando, el control y las comunicaciones (C^3) que en cualquier otra área (Medeiros, 2024).

Uno de los principales desafíos de las redes actuales es la interconexión de tecnologías de enlace utilizadas en tiempo real, sin pérdida de capacidad, alcance ni movilidad. Por consiguiente, un sistema de comunicaciones militar "debe ser una única estructura lógica integrada por múltiples tecnologías de enlace" (Camilo; Moura; Salles, 2020, p. 6). De hecho, entre las redes de comunicaciones que se utilizan actualmente en las subredes que componen la ROD —Recim, EBNet e Intraer—, las cuales emplean tecnologías del mercado, no existe la posibilidad de una integración automática y sin intervención humana, ya que fueron planeadas, implementadas y desarrolladas de manera orgánica e independiente. Esto hace que estén conectadas mediante enlaces específicos y adaptaciones limitadas a redes heredadas inconexas, con restricciones de interoperabilidad e integración incompleta, además de requerir la traducción de direcciones IP y puertos de red (NAT/PAT).

La ROD, como parte del SMDC, es uno de los pilares de la protección cibernética, que es una actividad de carácter permanente y tiene como objetivo mantener el funcionamiento

seguro y oportuno de los equipos y sistemas informáticos, así como promover la protección contra las acciones de explotación y los ataques del adversario (Brasil, 2023b). Dicho esto, gestionar una infraestructura de tal envergadura sin un liderazgo único y sin acciones coordinadas y alineadas —con el objetivo de converger en una infraestructura única— constituye un gran desafío.

4 UNA NUEVA VISIÓN PARA LA INTEGRACIÓN DE LA RED OPERACIONAL DE DEFENSA

La Doctrina Militar de Defensa Cibernética afirma que:

> El SMDC es un conjunto de instalaciones, equipos, doctrina, procedimientos, tecnologías, servicios y personal esenciales para llevar a cabo acciones destinadas a garantizar el uso efectivo del ciberespacio por parte de la Defensa Nacional, así como para impedir o dificultar acciones hostiles contra sus intereses. También le corresponde al SMDC garantizar la protección cibernética del SisMC², lo que permite actuar en red de manera segura, así como de forma integrada y colaborativa en la gestión de riesgos relacionados con la protección de infraestructuras críticas, tal como se establece en el Plan Nacional de Seguridad de Infraestructuras Críticas (Brasil, 2023b, p. 27).

En este sentido, la ciberseguridad ya avanza hacia una gestión integrada entre la MB, el EB y la FAB, pero aún no se refleja, en la práctica, en una infraestructura de conectividad e intercambio de datos conjuntos, supervisada por un único *Network Operation Center* (NOC) y por un *Security Operation Center* (SOC) —Centro de Operaciones de Red y de Seguridad, respectivamente—, lo cual permitiría consolidar todo este sistema.

4.1 Integración a nivel de personas, procesos y tecnologías

La Estrategia Nacional de Defensa afirma que:

> [...] se vuelve imperativo crear y ampliar polos tecnológicos integradores, con el objetivo de alcanzar la autosuficiencia en proyectos de desarrollo y en la fabricación de sistemas de C³I (Comando, Control, Comunicación e Inteligencia), con miras a eliminar, progresivamente, la dependencia externa (Brasil, 2025a, p. 14).

De este modo, esta propuesta tiene como objetivo presentar un modelo de innovación para la ROD, coordinando e integrando a las personas, los procesos y las tecnologías.

4.1.1 Propuesta de integración personal

Las medidas de protección cibernética son más efectivas cuando se alinean con otras dos variables que conforman el sistema de C² en acción: el personal y la doctrina, que, cuando son débiles, se convierten en vulnerabilidades potenciales (Cordeiro, 2014). Por lo tanto, corresponde

a las FFAA desarrollar una doctrina conjunta para que su personal esté capacitado y pueda difundir conocimientos, proteger las informaciones críticas, hacer frente a las acciones cibernéticas del adversario y mantenerse en condiciones de responder a los ataques.

En el ámbito de la integración personal, se pueden adoptar medidas drásticas y disruptivas, como la creación de una nueva Fuerza, o medidas más suaves e integradoras, similares a la creación del ComDCiber (Ministério de Defesa, 2016), en la que el MD y su EMCFA cuentan con experiencia en establecer proyectos y grupos de trabajo, estudiar y emitir directrices, y coordinar de manera continua. Dado que los efectivos de las Fuerzas no son proporcionales y que el EB está designado como responsable de la seguridad cibernética, una alternativa en este ámbito sería la creación de un nuevo Centro Conjunto de Operaciones de Red y Seguridad, con una actuación continua e integrada que, además de monitorear y operar la infraestructura de la ROD, participaría activamente en el diseño, desarrollo, implementación y soporte de una infraestructura de red única y común para desarrollar nuevas capacidades integradas.

La implementación de una infraestructura basada en redes definidas por software (SD-WAN) y la orquestación cognitiva exige una reestructuración profunda de las competencias del personal técnico de las Fuerzas Singulares. La transición del paradigma de configuración estática de activos a la gestión de flujos dinámicos requiere la capacitación de militares con el perfil de "Orquestadores de Redes" (paradigma NetOps). En este contexto, la alfabetización en Inteligencia Artificial Explicable (XAI) se convierte en un requisito fundamental, ya que permite al operador interpretar y validar las decisiones autónomas de los agentes de enrutamiento, garantizando que la automatización tecnológica permanezca bajo el control y la supervisión ética del responsable humano de la toma de decisiones en situaciones de crisis.

Además de la capacidad técnica, la "Nueva Visión" de la ROD supone una evolución en la cultura organizacional, pasando de los silos de información específicos de cada Fuerza a una mentalidad de plena interoperabilidad (*joint mindset*). Este cambio cultural es la base para que la soberanía digital se perciba como un activo colectivo. La confianza mutua en los protocolos de seguridad y el uso compartido de infraestructuras críticas bajo la coordinación del EMCFA permiten que la red actúe como un multiplicador del poder de combate, en el que la resiliencia del sistema trasciende las fronteras administrativas de cada Fuerza Individual.

La principal necesidad de aumentar la compatibilidad se satisface mediante un órgano conjunto de elaboración y mediación de requisitos operativos (Medeiros, 2024), que sería un punto de control único para la ROD, con un enfoque de gestión y supervisión de la red. Este grupo podría ser una subsección del ComDCiber, dedicada a la protección de las comunicaciones, los datos y la información; sin embargo, una solución más lógica y menos traumática sería la ampliación del NOC/SOC del SisTEx en Brasilia/DF, que actualmente administra casi mil sitios a nivel nacional. De este modo, sería posible la integración y absorción de Recim e Intraer por parte de EBNet, que se convertiría en la nueva ROD, con la colaboración del personal y los recursos financieros de la MB y la FAB, integrando por completo las unidades operativas de todas las Fuerzas Singulares. No es casualidad que el CITEx haya buscado una actualización tecnológica de EBNet a nivel nacional desde 2024 e, incluso, ya haya validado el uso de sus recursos en el contexto de las inundaciones de Río Grande del Sur — como se expondrá en la sección 4.2 de este artículo — y, desde entonces, cuente con el mayor número de militares capacitados en esta tecnología.

4.1.2 Propuesta de integración procesal

La integración y la estandarización de los procesos entre las FFAA tienden a ser eficaces, lo que permite combinar y actualizar las mejores prácticas, así como uniformar las regulaciones entre las Fuerzas Singulares, lo cual reduce las diferencias inherentes entre la MB, el EB y la FAB. Esta dinámica contribuye a acercar a las personas y a lograr la igualdad en las rutinas militares, lo que permite la planificación y las adquisiciones conjuntas, así como el desarrollo de capacidades y sistemas para la nueva ROD.

A nivel normativo, una actualización combinada no solo podría optimizar los procesos vigentes, sino también impulsar nuevas acciones estratégicas integradoras a nivel de red y de sistemas, ampliando el SMDC y armonizando las gestiones, las prácticas y las posibilidades en todos los niveles estratégicos, tácticos y operativos. Además, la concentración de datos militares puede generar la capacidad de ampliar la identificación de la información de inteligencia, correlacionar bases de datos y eventos de red, así como agregar repositorios de conocimiento e información conjunta.

Además, la concentración de datos militares puede generar la capacidad de ampliar la identificación de la información de inteligencia, correlacionar bases de datos y eventos de red, así como agregar repositorios de conocimiento e información conjunta (Força Aérea Brasileira, 2015). Si el MD prefiere ampliar las funciones de este órgano central de la red y añadirle nuevas atribuciones, esto puede establecerse mediante una nueva doctrina.

Otro proceso que se vería beneficiado sería la adquisición centralizada. En 2024, el CITEx realizó una compra de más de 800 equipos para su implementación en todo el territorio nacional, con un gran ahorro gracias al interés directo de los grandes fabricantes y a la economía de escala inherente. La centralización de las adquisiciones puede generar ganancias en eficacia y eficiencia para la Administración Pública Federal (APF), siempre y cuando se cuente con una mayor integración de los procesos de planificación de las tres Fuerzas, mediante la realización de compras conjuntas, una mayor estandarización del material y el incremento de la interoperabilidad entre ellas (Medeiros, 2024).

La propia orientación hacia el alojamiento de los sitios web y los sistemas de la MB y la FAB en los *data centers* del EB puede aumentar la eficacia en el uso de los recursos públicos, al compartir recursos militares y equipos de manejo de incidentes de red, entre otros. Esta solución se simplificaría y facilitaría aún más con la nueva ROD, que proporcionaría acceso a los sistemas nacionales de C^3I y a los conjuntos subordinados al MD.

En el ámbito de la gobernanza, la arquitectura propuesta optimiza la relación entre el nivel estratégico (EMCFA) y el operativo (Fuerzas Singulares) mediante el modelo de Redes Basadas en la Intención (IBN, por sus siglas en inglés). Este proceso permite que el comando superior establezca políticas de alto nivel, como la priorización del tráfico de comando y control en zonas de conflicto, mientras que la orquestación automatizada traduce esas intenciones en configuraciones técnicas en tiempo real. Este flujo de gobernanza preserva la autonomía operativa de las Fuerzas en el frente, al tiempo que garantiza la conformidad sistémica y la agilidad en la respuesta a incidentes jurisdiccionales.

Desde el punto de vista teórico, la integración de los procesos de *Zero Trust Architecture* (ZTA) redefine el flujo de acceso a los datos estratégicos, sustituyendo la confianza basada en el perímetro por una verificación continua de la identidad y la integridad. Este rigor procesal se ve potenciado por la segmentación de la red (*network slicing*), que permite el aprovisionamiento *on*

demand de redes lógicas aisladas para misiones específicas. De esta manera, la ROD pasa de ser una infraestructura rígida a un servicio flexible y resiliente, capaz de crear corredores seguros de comunicación en teatros de operaciones dinámicos, con una agilidad superior a la de los procesos tradicionales de ingeniería de tráfico.

4.1.3 Propuesta de integración tecnológica

En el ámbito tecnológico, se están estudiando redes empresariales atractivas (Navarro; Canonico; Botta, 2023), más autónomas e inteligentes, que pueden adaptarse y recuperarse por sí mismas con menor interacción humana (Waseem *et al*., 2022), lo que aporta mayor resiliencia, reduce los costos y permite la adopción de alternativas de mercado completas para la nueva ROD. Entre ellas, algunas pueden ofrecer un nuevo modelo de arquitectura de red definida por software, programable y flexible (*Aggarwal*, 2020) para entornos locales (*Local Area Network* – LAN), mediante Software Defined Networks (SDN), o de larga distancia (*Wide Area Network* – WAN), mediante SD-WAN. Esta evolución desarrolla capacidades computacionales (Khalifa *et al*., 2025) e innovaciones continuas gracias a una amplia investigación (Belgaum *et al*., 2020).

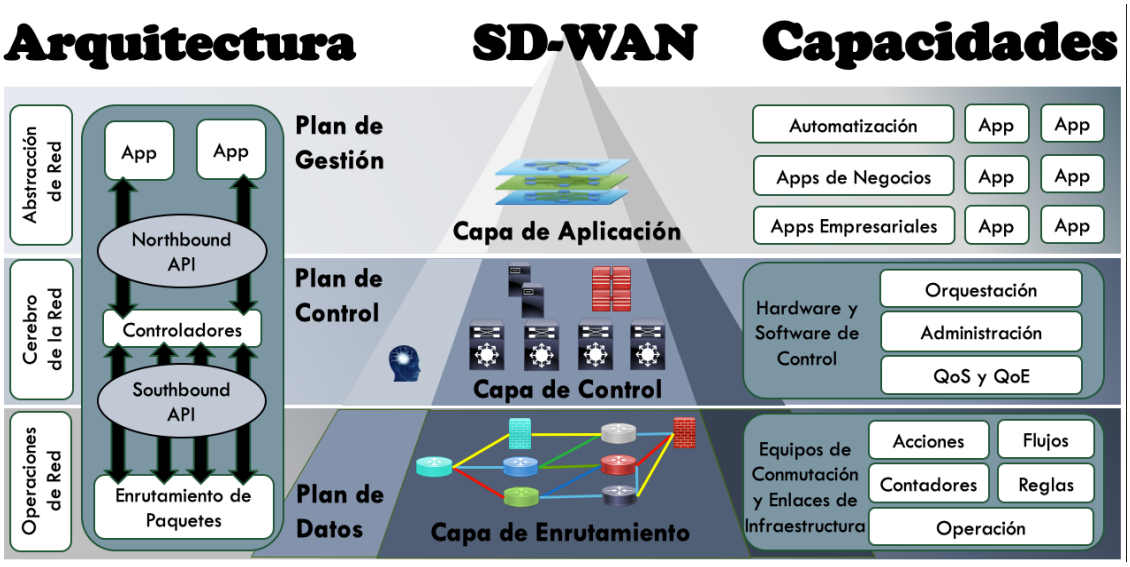
Debido a la extensión continental de Brasil y al amplio ámbito de actuación de las FFAA, la arquitectura de redes de comunicaciones SD-WAN puede operar a escala global, como una tecnología de red flexible ampliamente utilizada en la actualidad (Fu; Wang; Wang, 2024). Consiste en una solución basada en un conjunto programable de hardware y software con ventajas tales como: bajo costo, gracias a la reducción de los requisitos de hardware y los gastos operativos (Díaz *et al*., 2022); mayor velocidad y gestión simplificada; mayor seguridad y visibilidad, con análisis detallados y automatización en la resolución de problemas; mayor disponibilidad, mediante un *failover* simplificado y rápido; y mejor rendimiento general de la red, con optimización del ancho de banda (Yalda; Hamad; Tapus, 2022). Esta tecnología se presenta como un medio capaz de satisfacer los requisitos necesarios para alcanzar los objetivos nacionales de defensa.

La ingeniería innovadora integrada permite reducir los costos recurrentes de los sistemas, ofrecer un amplio control y visibilidad, y mejorar la innovación en la organización de la infraestructura de manera automatizada mediante una administración integrada (Badotra; Panda, 2020). Cabe destacar que el EB ya cuenta con experiencia en la tecnología SD-WAN. Actualmente, el CITEx utiliza recursos del Programa de Defensa Cibernética con el objetivo de dotar al EB de capacidades para actuar en el espacio cibernético a nivel estratégico, operativo y táctico (Estado-Maior do Exército, 2022). Entre las próximas medidas se encuentra la reestructuración de la protección cibernética de EBNet (Oliveira; Teixeira, 2021), con gran parte de los recursos destinados a esta solución. Proyectos paralelos, como el Sistema Integrado de Monitoreo de Fronteras (Sisfron), también tienen como objetivo la adquisición de equipos de TI para los centros de operaciones ubicados en la zona fronteriza (Exército Brasileiro, 2024c) y contribuyen a la ejecución de las adquisiciones y a la coordinación de las entregas.

Entre los pilares estratégicos de los proyectos futuros, recogidos en las numerosas doctrinas actualizadas recientemente y citadas en este artículo, se destacaron como premisas la flexibilidad y la unidad. La tecnología de redes que mejor cumple con estos requisitos a nivel nacional, y que puede expandirse a nivel global, es el SD-WAN, cuya arquitectura y capacidades se muestran

en la Figura 2. Esta tecnología aprovecha la flexibilidad y la programabilidad de una SDN (Abderrahman *et al*., 2023), además de ofrecer una visión global de todas las sedes e integrar la red en todos los niveles. Esta solución también permite que todas las políticas de gestión y control de la red vigentes se implementen simultáneamente (Ouamri *et al*., 2025), además de hacer posible la segregación y la migración hacia una implementación gradual supervisada por sitio u OM.

Figura 2 – Arquitectura general de la tecnología SD-WAN y sus capacidades.



Fuente: Elaborada por el autor.

El Plan de Gestión de SD-WAN conserva las aplicaciones de SDN (Kaur; Krishna; Patil, 2025) e incorpora otras nuevas, orientadas a los objetivos comerciales, organizacionales o empresariales, lo que permite una gestión simplificada de la red y de los dispositivos vinculados a ella (Mahar *et al*., 2024) y aumenta el nivel de gestión y control de las sucursales y los sitios remotos vinculados. De manera similar, coordina las configuraciones y políticas de red que el plan de control debe implementar en el entorno de producción empresarial (Ali *et al.*, 2015).

El Plan de Control también se encarga de la administración del Plan de Datos (Bahashwan *et al*., 2023), pero requiere una mayor resiliencia debido a cuestiones de distancia y métricas relacionadas que pueden interrumpir la comunicación con un único controlador remoto. De esta manera, la latencia o el retraso pueden afectar negativamente la administración y la configuración de flujos y reglas, así como las fallas en los enlaces pueden afectar el control y dejar la red inoperante (Ayodele; Buttigieg, 2024). Por ese motivo, es común implementar más de un controlador distribuido para lograr una mayor resiliencia del control y una mayor eficiencia en el enrutamiento (Kanwal *et al.*, 2024). Para que esto sea posible, se requiere una coordinación adicional entre los controladores, manteniéndolos siempre coordinados y sincronizados, lo que permite la conectividad con la QoS (Calidad de Servicio) y la QoE (Calidad de Experiencia) previstas (Rahouti *et al.*, 2022).

El plano de datos del SD-WAN ejecuta los enrutamientos de la solución en una infraestructura compleja y distribuida, con múltiples enlaces de red simultáneos y redundantes entre los nodos y las sedes, mediante las más diversas tecnologías (Rahouti; Xiong; Xin, 2020). Dicho esto, existe una subdivisión en la capa de enrutamiento entre la red de infraestructura y una malla lógica de nivel superior, que crea túneles específicos y alternativos con reglas de enrutamiento granularizadas y encriptadas de punto a punto dentro de la organización (Abdi *et al.*, 2024).

La solución SD-WAN se considera flexible y única porque utiliza capas de abstracción y elementos optimizados para WAN a fin de ofrecer dichas capacidades, las cuales conforman un único sistema (Jiménez *et al.*, 2021). Su administración la realiza el Orquestador de Servicios de la solución, que actúa como una capa superior y administra múltiples controladores SD-WAN y aplicaciones de negocios (Jain; Khondoker, 2018). Se encarga de simplificar la configuración y la administración de políticas en una red distribuida geográficamente. Los equipos de conmutación distribuidos son los *Customer Premises Equipment* (CPE), dispositivos físicos o virtuales de borde implementados en sucursales, centros de datos y nubes. Son los puntos de inicio y fin de los túneles SD-WAN y se encargan de encapsular el tráfico y aplicar las políticas. Los Túneles de Superposición (*overlay*) son túneles seguros —como el *Protocol Security* (IPSec) o la *Virtual Extensible* LAN (VXLAN)— sobre redes físicas subyacentes (*underlay*) para crear una red virtual y privada. Esto permite el uso de diversas opciones de conectividad y garantiza la seguridad en redes públicas (Kytomäki, 2021).

Por lo tanto, el SD-WAN está diseñado para administrar redes WAN que conectan múltiples sitios geográficamente dispersos, como filiales de empresas, *data centers* e infraestructuras de nube pública o privada. Su objetivo es optimizar la conectividad a través de múltiples redes subyacentes (MPLS, Internet, 4G/5G, satélites) con el fin de garantizar una alta calidad de servicio (QoS) y una excelente experiencia (QoE), además de seguridad y reducción de costos (Badotra; Panda, 2020). En resumen, mientras que la SDN sienta las bases de una red programable y centralizada, el SD-WAN la amplía y la optimiza para las complejidades y exigencias de las redes de larga distancia modernas, incorporando capas adicionales de funcionalidad e inteligencia (Rahman; Hasan; Jeong, 2022). En este momento en que contamos con inteligencia y una visión centralizada de la red, la combinación con soluciones de IA aumenta su relevancia (Sahran; Altarturi; Anuar, 2024).

Actualmente, Recim encripta los datos y utiliza enlaces redundantes, además de monitorear constantemente los sistemas críticos (Marinha do Brasil, 2025). El SD-WAN puede garantizar la continuidad de estos servicios, ya que permite seleccionar múltiples enlaces de manera automática, encriptando los sitios de forma automatizada y coordinada, con filtros de control específicos por flujos, siempre que estén autorizados por las políticas vigentes. De este modo, aporta solidez más allá de la infraestructura propia de las Fuerzas Armadas, mediante el uso de medidas avanzadas de seguridad y recursos para prevenir y responder a las amenazas cibernéticas, con el fin de maximizar la resiliencia frente a los desafíos de la guerra cibernética moderna.

Aunque la tecnología SD-WAN ofrece un gran potencial de automatización y reducción de costos operativos, su implementación en la ROD plantea desafíos significativos. La transición de redes heredadas y fragmentadas a una estructura única exige una gobernanza interinstitucional sólida para evitar conflictos de gestión entre las Fuerzas Singulares. Además, la interoperabilidad entre diferentes fabricantes —lo que evita el *vendor lock-in*— y la necesidad de capacitación

continua del personal técnico para manejar redes programables son obstáculos que exigen una planificación de transición gradual y supervisada.

Por último, para superar los retos de implementación y mitigar las limitaciones mencionadas, es imprescindible fomentar la autonomía tecnológica y la soberanía digital. En este contexto, la transición hacia una ROD moderna e integrada exige impulsar el desarrollo de soluciones SD-WAN de soberanía nacional, coordinadas bajo el modelo de innovación de la Triple Hélice (Estado, Academia e Industria). La convergencia de esfuerzos entre los institutos de investigación de las Fuerzas Armadas, las universidades y la Base Industrial de Defensa (BID) es esencial para reducir la dependencia estratégica de tecnologías y protocolos extranjeros. Esta coordinación no solo fortalece la innovación en el sector de la defensa, sino que también garantiza que el control y la gobernanza de la infraestructura crítica de comunicaciones del país permanezcan bajo estricta jurisdicción y dominio tecnológico nacional.

4.2 Validación del SD-WAN durante las inundaciones en el estado de Rio Grande do Sul y la evolución tecnológica de EBNet

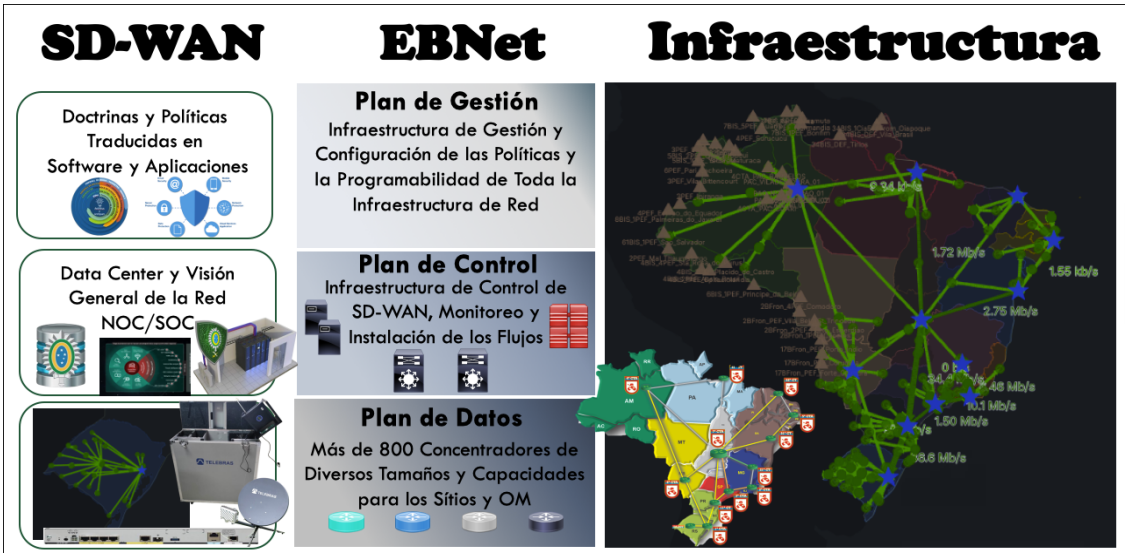
Con motivo de las fuertes inundaciones que se produjeron en el sur de Brasil en 2024 y que dieron lugar a la Operación Taquari II, la infraestructura de C^2 sufrió una gran inestabilidad. Ante las interrupciones consecutivas, simultáneas y prolongadas de los medios convencionales de red y conectividad, faltaron militares técnicos calificados para actuar en los cambios necesarios para la supervivencia de la red. Era necesario realizar ajustes en la configuración de los equipos para encriptar los enlaces convencionales, que presentaban interrupciones, así como para configurar los túneles para distintos sitios, lo cual se hacía manualmente y en un contexto de escasa disponibilidad de recursos, como transporte y energía eléctrica.

Como alternativa, se convirtieron los enlaces Metro Ethernet a Internet, lo que aumentó su disponibilidad. Además, se recibieron y distribuyeron en el estado más de 480 terminales satelitales de diferentes tecnologías para las OM y los puestos tácticos, lo que permitió a los usuarios acceder de forma remota a EBNet mediante el uso de un cliente VPN en los dispositivos. Para garantizar respuestas más rápidas e independientes de la interacción humana, se realizó de manera urgente la implementación virtual del software integrador de SD-WAN, el cual concentró las políticas de enrutamiento encargadas de coordinar y controlar los flujos de red entre los equipos utilizados en esta arquitectura en tres sitios críticos de EBNet, los cuales operaron en paralelo y concentraron todos los enlaces disponibles en esa OM (Metro Ethernet, radio, fibra, Internet y satélite). La nueva solución logró monitorear, seleccionar y enrutar los paquetes de red con los recursos existentes, realizando un equilibrio de carga automatizado entre los enlaces disponibles y seleccionando la ruta recomendada por las políticas vigentes preconfiguradas, lo que aumentó la resiliencia de las redes y permitió un flujo continuo de información. De este modo, gracias a la implementación rápida, eficaz y parcialmente virtualizada de la infraestructura SD-WAN en sitios estratégicos (Figura 3), se logró la integración completa y segura de las redes internas de las unidades operativas, lo que validó gran parte de las ventajas expuestas en este artículo.

En la Figura 3, se puede identificar la composición de las capas SD-WAN integradas a EBNet en la prueba piloto, lo que traduce las doctrinas y políticas en software. Estos están orientados a una inteligencia computacional que concentra toda la información de la red y la conecta de

manera adecuada a los mejores enlaces disponibles, incluyendo medios provisionales y dinámicos, como es el caso de los recursos de emergencia de los enlaces satelitales. Las OM del Sur fueron pioneras en el proceso de migración de todo el Ejército, durante la ejecución del Proyecto de Protección del Entorno Cibernético. El SisTEx continúa diseñando, implementando y operando en todo el territorio nacional, con el apoyo regional de los Centros de Telemática.

Figura 3 – Infraestructura de validación de SD-WAN en las Inundaciones del Sur



Fuente: Elaborada por el autor.

De esta manera, se puede afirmar que el SD-WAN fue eficaz en la integración de las OM con flexibilidad y resiliencia en EBNet, lo que garantizó el éxito en la gestión automatizada de los enlaces mediante software y permitió concluir que esta era la mejor solución tecnológica para momentos de incertidumbre. Esta herramienta proporcionó conectividad y seguridad gracias a la programabilidad de las políticas, lo que amplió la autonomía de la red, hizo posible el *self-healing* (autorreparación), automatizó los flujos de datos y requirió menos atención por parte del equipo técnico especializado ante las interrupciones en los enlaces de infraestructura.

El CITEx ya estaba diseñando una red como esta, más autónoma y flexible; sin embargo, no se implementó antes de que ocurriera este desastre, que terminó siendo una prueba de la eficiencia de la tecnología SD-WAN incluso en redes extensas como las del EB, con más de 860 puntos de conexión. Este hecho fue fundamental para las adquisiciones subsiguientes, que ya se habían planeado a nivel nacional y que cuentan con un proceso de licitación estandarizado y centralizado, el cual es válido a nivel nacional y permite ofrecer una visión global e integrada para la nueva EBNet. En los meses siguientes, el EB logró acelerar las etapas del proyecto de evolución tecnológica de EBNet y redirigir los equipos fabricados inicialmente hacia la región sur, lo que permitió implementar y poner en funcionamiento esta tecnología en los 108 cuarteles regionales en unos pocos meses, lo cual aumentó la capacidad de supervivencia en la región. En este contexto, se deduce que dicha infraestructura

puede expandirse de manera orgánica e incorporar más sitios, incluidos los de la MB y la FAB, con el fin de constituir la nueva ROD e integrar a las personas, los procesos y los servicios.

5 CONSIDERACIONES FINALES

El EME definió la Fuerza 40 para guiar la evolución del Concepto de Transformación del EB en el período comprendido entre 2024 y 2039, basada y fundamentada en los siguientes ejes de trabajo: Concepto Estratégico orientado hacia 2040; nuevas capacidades; nueva doctrina; y nuevo personal (Exército Brasileiro, 2024d). En este contexto, la propuesta desarrollada para la nueva ROD surge en el momento oportuno, ya que incorpora capacidades de Protección y Defensa Cibernéticas y le otorga al EB el protagonismo para asumir el papel de coordinador de la infraestructura conjunta de las FFAA.

En un contexto de recursos financieros escasos y dependencia tecnológica, en el que existe la necesidad de adquirir tecnología extranjera de manera inmediata, no hay nada más deseable que adoptar un modelo único de infraestructura flexible y capaz de mejorar la integración de las redes y los sistemas en todos los niveles, lo que permite el desarrollo de capacidades conjuntas. Además, cuanto antes se establezcan alianzas estratégicas con un país aliado con el que se compartan intereses comunes, antes podrá Brasil desarrollar su propia tecnología de SD-WAN. Esta solución ofrece programabilidad y flexibilidad gestionadas por software, y se ve totalmente potenciada por avances paralelos y capacidades agregadas por la IA (Cifuentes *et al.*, 2024).

En este sentido, la Estrategia Brasileña de Inteligencia Artificial (EBIA) (Brasil, 2021) afirma que la integración de los sistemas de IA en la estructura productiva es una realidad, y que desempeñará un papel fundamental para mejorar la eficacia, reducir costos y minimizar los errores operativos, además de automatizar una serie de procesos y hacer que las rutinas sean más flexibles y ágiles. En total consonancia con ello, se elaboró para el EB una directriz estratégica que recomienda implementar e integrar sistemas de IA, lo que permite procesar información procedente de diversas fuentes existentes, así como estructurar y relacionar los datos proporcionados por nuevos sensores y sistemas, con el objetivo de generar una conciencia situacional oportuna, anticipar eventos y apoyar la toma de decisiones (Exército Brasileiro, 2024e). De manera conjunta, también surge la oportunidad de ampliar, optimizar y compartir las inversiones en infraestructura de IA de las FFAA y del MD.

REFERENCIAS

ABDERRAHMAN, R. *et al*. Software Defined Networking Concept (SDN) Based on Artificial Intelligence: Taxonomy of Methods and Future Directions. **Springer Nature**, Switzerland, 2023.

ABDI, A. H. *et al*. Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions. **IEEE Access**, 2024.

AGGARWAL, A. Artificial Intelligence in Software Defined Networking. **International Journal of Advance Research, Ideas and Innovations in Technology**, v. 6, n. 2, 2020.

ALI, S. T. *et al*. A Survey of Securing Networks Using Software Defined Networking. **IEEE Transactions on Reliability**, v. 64, n. 3, 2015.

AYODELE, B.; BUTTLGLEG, V. SDN as a defence mechanism: a comprehensive survey. **International Journal of Information Security**, v. 23, p. 141-185, 2024.

BADOTRA, S.; PANDA, S. N. A Survey on Software Defined Wide Area Network. **International Journal of Applied Science and Engineering**, 2020.

BAHASHWAN, A. A. *et al*. A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking. **Sensors**, v. 23, n. 9, p. 4441, 2023.

BELGAUM, M. R. *et al*. A Systematic Review of Load Balancing Techniques in Software-Defined Networking. **IEEE Access**, 2020.

BRASIL. Ministério da Defesa. **Doutrina para o Sistema Militar de Comando e Controle (MD31-M-03)**. Brasília, DF: Ministério da Defesa, 2015. Disponible en: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/doutrina_militar/lista_de_publicacoes/md31a_ma_03a_douta_sismca_3a_eda_2015.pdf. Accedido en: 22 jul. 2025.

BRASIL. **Comando Conjunto na Defesa Cibernética**. Agência Gov Br, 2017. Disponible en: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/ultimas-noticias/comando-conjunto-na-defesa-cibernetica. Accedido en: 25 jul. 2025.

BRASIL. Ministério da Defesa. **Conceito Operacional (CONOPS) do Sistema de Informação e de Apoio à Decisão para Comando e Controle (SIADC²) – MD31-S-04**. 1. ed. Brasília, DF: Ministério da Defesa, 2019. Disponible en: https://www.gov.br/defesa/pt-br/arquivos/File/doutrinamilitar/listadepublicacoesEMD/md31a_sa_04a_finala_20a_nova_2019a_1a_edicao.pdf. Accedido en: 21 jul. 2025.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas (MD30-M-01)**. Brasília, DF: Ministério da Defesa, 2020. Disponible en: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/legislacao/emcfa/publicacoes/doutrina/md30-m-01-vol-1-2a-edicao-2020-dou-178-de-15-set.pdf. Accedido en: 22 jul. 2025.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. **Estratégia Brasileira de Inteligência Artificial (EBIA)**. Brasília, DF: MCTI, 2021. Disponible en: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/copy2_of_RelatoriofinalEBIA_Eixo6V2.4.pdf. Accedido en: 8 jul. 2026.

BRASIL. Ministério da Defesa. **Política de Segurança da Informação para o Sistema Militar de ComandoeControle**. Brasília, DF: Ministério da Defesa, 2023a. Disponibleen:https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31P03PolticadeSeguranadaInformaoparaoSistemaMilitardeComandoeControle3Ed2023.pdf. Accedido en: 21 jul. 2025.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética (MD31-M-07)**. Brasília, DF: Ministério da Defesa, 2023b. Disponible en: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Accedido en: 27 jul. 2025.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa (END)**. Brasília, DF: Ministério da Defesa, 2025a. Disponible en: https://www.gov.br/defesa/pt-br/acesso-a-informacao/governanca/governanca-do-setor-de-defesa/decreto-no-12-725-de-18-de-novembro-de-2025-dou_lbdn.pdf. Accedido en: 24 jul. 2025.

BRASIL. Ministério da Defesa. **Planejamento Estratégico Setorial de Defesa (PESD) 2024-2035**. Brasília, DF: Assessoria Especial de Planejamento, 2025b. Disponible en: https://www.gov.br/defesa/pt-br/acesso-a-informacao/governanca/governanca-do-setor-de-defesa/planejamento-estrategico-1/arquivos/2025/web_planejamento-estrategico-setorial-de-defesa.pdf. Accedido en: 24 jul. 2025.

CAMILO, J. M.; MOURA, D. F. C.; SALLES, R. M. Redes de comunicações militares: desafios tecnológicos e propostas para atendimento dos requisitos operacionais do Exército Brasileiro. **Revista Militar de Ciência e Tecnologia (RMCT)**, v. 37, n. 3, 2020.

CIFUENTES, B. J. O. *et al*. Analysis of the Use of Artificial Intelligence in Software-Defined Intelligent Networks: A Survey. **Technologies**, v. 12, n. 7, p. 99, 2024.

CORDEIRO, S. S. **A influência da Guerra Cibernética nos sistemas de Comando e Controle (C2) nas Operações Militares**. [*s. l.*]: Escola de Comando e Estado-Maior do Exército, 2014.

DIAZ, C. J. M. *et al*. Analysis about Benefits of Software-Defined Wide Area Network: A New Alternative for WAN Connectivity. **International Journal of Advanced Computer Science and Applications (IJACSA)**, v. 13, n. 1, 2022.

ESTADO MAIOR DO EXÉRCITO. **Os projetos/programas estratégicos do EB**: importância, situação atual e perspectivas. Brasília, DF: Escritório de Projetos do Exército, 2022. Disponible en: https://epex.eb.mil.br/index.php/programas-estrategicos-do-exercito. Accedido en: 27 jul. /2025.

ESTADOS UNIDOS DA AMÉRICA. Joint Staff. **Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System**. Washington, DC: Joint Staff, 2021. Disponible en: https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%205123.01J.pdf.Accedido en: 22 jul. 2025.

ESTADOS UNIDOS DA AMÉRICA. Department of Defense. **Summary of TI-IE Joint All-Domain Command & Control (JADC2) Strategy**. Washington, DC: Department of Defense, 2022. Disponible en: https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf. Accedido en: 22 jul. 2025.

EXÉRCITO BRASILEIRO. Secretaria Geral do Exército. **Instruções Gerais para Estruturação e Emprego Sistêmico da Base de Dados Corporativa do Exército Brasileiro (EBCORP), - EB10-IG-01.005**. 1. ed. Brasília, DF: SGEx, 2013. Disponible en: https://www.sgex.eb.mil.br/sg8/002_instrucoes_gerais_reguladoras/01_gerais/port_n_578_cmdo_eb_10jul2013.html. Accedido en: 25 jul. 2025.

EXÉRCITO BRASILEIRO. Secretaria Geral do Exército. **Diretriz Estratégica Organizadora do Sistema de Comando e Controle do Exército (EB10-D-01.013)**. 2. ed. Brasília, DF: Secretaria Geral do Exército, 2021. Disponible en: https://www.sgex.eb.mil.br/sg8/002_instrucoes_gerais_reguladoras/01_gerais/port_n_578_cmdo_eb_10jul2013.html. Accedido en: 8 jul. 2026.

EXÉRCITO BRASILEIRO. Secretaria Geral do Exército. **Diretriz Organizadora do Sistema Estratégico de Comando e Controle do Exército (EB20-D-02.037)**. 1. ed. **Secretaria Geral do Exército**, 2024a. Disponible en: https://www.sgex.eb.mil.br/sistemas/boletim_do_exercito/copiar.php?codarquivo=181261862&act=sep. Accedido en: 27 jul. 2025.

EXÉRCITO BRASILEIRO. Centro Integrado de Telemática do Exército (CITEx). **Missão, visão e valores**. Brasília, DF: CITEx, 2024b. Disponible en: https://citex.eb.mil.br/index.php/institucional/missao-visao-e-valores.html. Accedido en: 25 jul. 2025.

EXÉRCITO BRASILEIRO. Escritório de Projetos. **SISFRON**. Brasília, DF: Escritório de Projetos, 2024c. Disponible en: https://epex.eb.mil.br/. Accedido en: 27 jul. 2025.

EXÉRCITO BRASILEIRO. Comando do Exército. **Concepção de Transformação do Exército e do Desenho da Força 40 – 2024-2039 (EB10-P- 01.025)**. 1. ed. Brasília, DF: Comando do Exército, 2024d. Disponible en: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/07_publicacoes_diversas/01_comando_do_exercito/port_n_2300_cmdo_eb_12agosto2024.html. Accedido en: 27 jul. 2025.

EXÉRCITO BRASILEIRO. Estado-Maior do Exército (EME). **Diretriz Estratégica de Inteligência Artificial para o Exército Brasileiro**. Brasília, DF: EME, 2024e. Disponible en: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/04_estado-maior_do_exercito/port_n_1318_eme_14mai2024.html. Accedido en: 8 jul. 2026.

FORÇA AÉREA BRASILEIRA. Organização se prepara para proteger redes corporativas da instituição. **Tecnologia da Informação**, 2015. Disponible en: https://www.fab.mil.br/noticias/tag/DTI. Accedido en: 27 jul. /2025.

FORÇA AÉREA BRASILEIRA. Diretoria de Tecnologia da Informação completa 13 anos. **O Portal da FAB**, 2023. Disponible en: https://forcaaerea.fab.mil.br/noticias/mostra/40280/ANIVERS%C3%81RIO%20-%20Diretoria%20de%20Tecnologia%20da%20Informa%C3%A7%C3%A3o%20completa%2013%20anos. Accedido en: 21 jul. 2025.

FORÇA AÉREA BRASILEIRA. Centro de Defesa Cibernética encerra intercâmbio com expectativas superadas. **Agência da Força Aérea**, 2025. Disponible en: https://www.fab.mil.br/noticias/mostra/44014/DEFESA%20CIBERN%C3%89TICA%20-%20Centro%20de%20Defesa%20Cibern%C3%A9tica%20encerra%20interc%C3%A2mbio%20com%20expectativas%20superadas. Accedido en: 25 jul. /2025.

FU, C.; WANG, B.; WANG, W. Software-Defined Wide Area Networks (SD-WANs): A Survey. School of Computer Science and Technology, **Harbin Institute of Technology**, v. 13, n. 15, p. 3011, 2024.

JAIN, R.; KHONDOKER, R. Security Analysis of SDN WAN Applications - B4 and IWAN. *In*: KHONDOKER, R. SDN and NFV Security. [*s. l.*]: **Springer Lecture Notes in Networks and Systems**, v. 30, p. 111-127, 2018.

JIMÉNEZ, M. B. *et al*. A Survey of the Main Security Issues and Solutions for the SDN Architecture. **IEEE Access**, v. 9, p. 122016-122038, 2021.

KANWAL, A. *et al*. Exploring Security Dynamics in SDN Controller Architectures: Threat Landscape and Implications. **IEEE Access**, 2024.

KAUR, A.; KRISHNA, C. R.; PATIL, N. V. A comprehensive review on Software-Defined Networking (SDN) and DDoS attacks: Ecosystem, taxonomy, traffic engineering, challenges and research directions. **Computer Science Review**, v. 55, n. 9, p. 100692, 2025.

KHALIFA, E. H. *et al*. Brief Review of Using Machine Learning for Traffic Engineering in Software-Defined Networks. **Pakistan Journal of Life and Social Sciences**, v. 3, n. 1, p. 1738-1758, 2025.

KYTOMÄKI, J. **Artificial Intelligence and Machine Learning with SD-WAN**. 2021. Dissertação (Mestrado em Inteligência Artificial e Aprendizado de Máquina com SD-WAN) – [*s. l.*], 2021.

MAHAR, I. A. *et al*. A Comprehensive Survey of Software Defined Networking and its Security Threats. *In*: IEEE 1ST KARACHI SECTION HUMANITARIAN TECHNOLOGY CONFERENCE (KHI-HTC), 2024. **Anais** [...]. IEEE, 2024.

MARINHA DO BRASIL. Diretoria de Comunicação e Tecnologia da Informação da Marinha. **Acervo Arquivístico da Matinha do Brasil**, 2012. Disponible en: https://arquivodamarinha.marinha.mil.br/index.php/diretoria-de-comunicacao-e-tecnologia-da-informacao-da-marinha. Accedido en: 25 jul. 2025.

MARINHA DO BRASIL. Comunicações Navais: conheça a rede invisível que conecta e protege a Amazônia Azul. **Agência Marinha de Notícias**, 2025. Disponible en: https://www.agencia.marinha.mil.br/index.php/ciencia-e-tecnologia/comunicacoes-navais-conheca-rede-invisivel-que-conecta-e-protege-amazonia-azul. Accedido en: 21 jul. 2025.

MEDEIROS, F. A. R. **Organizações Conjuntas de Aquisição de Material de Defesa**: Uma alternativa para o Brasil? Rio de Janeiro: Biblioteca Digital do Exército, 2024. Disponible en: https://bdex.eb.mil.br/jspui/handle/123456789/13200. Accedido en: 8 jul. 2026.

MINISTÉRIO DA DEFESA. **Diretriz de Implantação do Projeto de Criação do Comando de Defesa Cibernética**. Brasília, DF: Exército Brasileiro, 2016. Disponible en: https://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/04_estado-maior_do_exercito/port_n_004_eme_08jan2016.html. Accedido en: 27 jul. 2025.

MINISTÉRIO DA DEFESA. **Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências**. Portaria nº 3.781/GM-MD, de 2020. Brasília, DF: Gabinete do Ministro, 2020. Disponible en: https://mdlegis.defesa.gov.br/norma_pdf/?NUM=3781&ANO=2020&SER=A. Accedido en: 27 jul. 2025.

NAVARRO, A.; CANONICO, R.; BOTTA, A. Software Defined Wide Area Networks: Current Challenges and Future Perspectives. *In*: INTERNATIONAL CONFERENCE ON NETWORK SOFTWARIZATION (NETSOFT), 9., 2023. **Anais** [...]. IEEE, 2023.

NETO, E. P. O Sistema de Comunicações Militares por Satélite do Brasil: breves considerações. **Panorâmico**, Rio de Janeiro, v. 2, n. 6, p. 61-64, 2023.

OLIVEIRA, M. M.; TEIXEIRA, L. **A defesa cibernética, o EB e a gestão de projetos**. Trabalho de Conclusão de Curso (Especialização em Gestão, Assessoramento e Estado-Maior) – Escola de Formação Complementar do Exército, Salvador, 2021.

OUAMRI, R. A. *et al*. A comprehensive survey on software-defined wide area network (SD-WAN): principles, opportunities and future challenges. **The Journal of Supercomputing**, v. 81, n. 291, 2025.

PEDERNEIRAS, L. C. **A guerra em transformação:** inteligência artificial sob a teoria de Clausewitz. Dissertação (Mestrado em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2024. Disponible en: https://bdex.eb.mil.br/jspui/handle/123456789/13882. Accedido en: 8 jul. 2026.

RAHMAN, A.; HASAN, K.; JEONG, S. H. An Enhanced Security Architecture for Industry 4.0 Applications based on Software-Defined Networking. *In*: INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATION TECHNOLOGY CONVERGENCE (ICTC), 13., 2022. **Anais** [...]. IEEE, 2022.

RAHOUTI, M. *et al*. SDN Security Review: Threat Taxonomy, Implications, and Open Challenges. **IEEE Access**, 2022.

RAHOUTI, M.; XIONG, K.; XIN, Y. Secure Software-Defined Networking Communication Systems for Smart Cities: Current Status, Challenges, and Trends. **IEEE Access**, 2020.

REINO UNIDO. Ministry of Defence. **Strategic Defence Review**: Making Britain Safer: secure at home, strong abroad. Londres: Ministry of Defense, 2025. Disponible en: https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad. Accedido en: 8 jul. 2026.

SAHRAN, F.; ALTARTURI, H. H. M.; ANUAR, N. B. Exploring the Landscape of AI-SDN: A Comprehensive Bibliometric Analysis and Future Perspectives. **Eletronics**, v. 13, n. 1, p. 26, 2024.

SANTOS, M. G.; OLIVEIRA, J. M. P.; BELDERRAIN, M. C. N. Estruturação do Problema de Dimensionamento de Enlaces EBNet com Value-Focused Thinking e Strategic Choice Approach. *In*: SIMPÓSIO DE GUERRA ELETRÔNICA (SIGE), 2022. Disponible en: https://www.sige.ita.br/aiovg_videos/estruturacao-do-problema-de-dimensionamento-de-enlaces-ebnet-com-value-focused-thinking-e-strategic-choice-approach/. Accedido en: 21 jul. 2025.

UCRÂNIA. Unmanned Systems Force. **Unmanned Systems Force**, 2025. Disponible en: https://usforces.army/en/. Accedido en: 21 jul. 2025.

WASEEM, Q. *et al*. Software-Defined Networking (SDN): A Review. In: INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICOIACT), 5., 2022. **Anais** [...]. IEEE, 2022.

YALDA, K. G.; HAMAD, D. J.; TAPUS, N. A survey on Software-defined Wide Area Network (SD-WAN) architectures. In: INTERNATIONAL CONGRESS ON HUMAN-COMPUTER INTERACTION, OPTIMIZATION AND ROBOTIC APPLICATIONS (HORA), 2022. **Anais** [...]. IEEE, 2022.