CRIPTOSISTEMAS PARA SECURIZAR LAS COMUNICACIONES TÁCTICAS

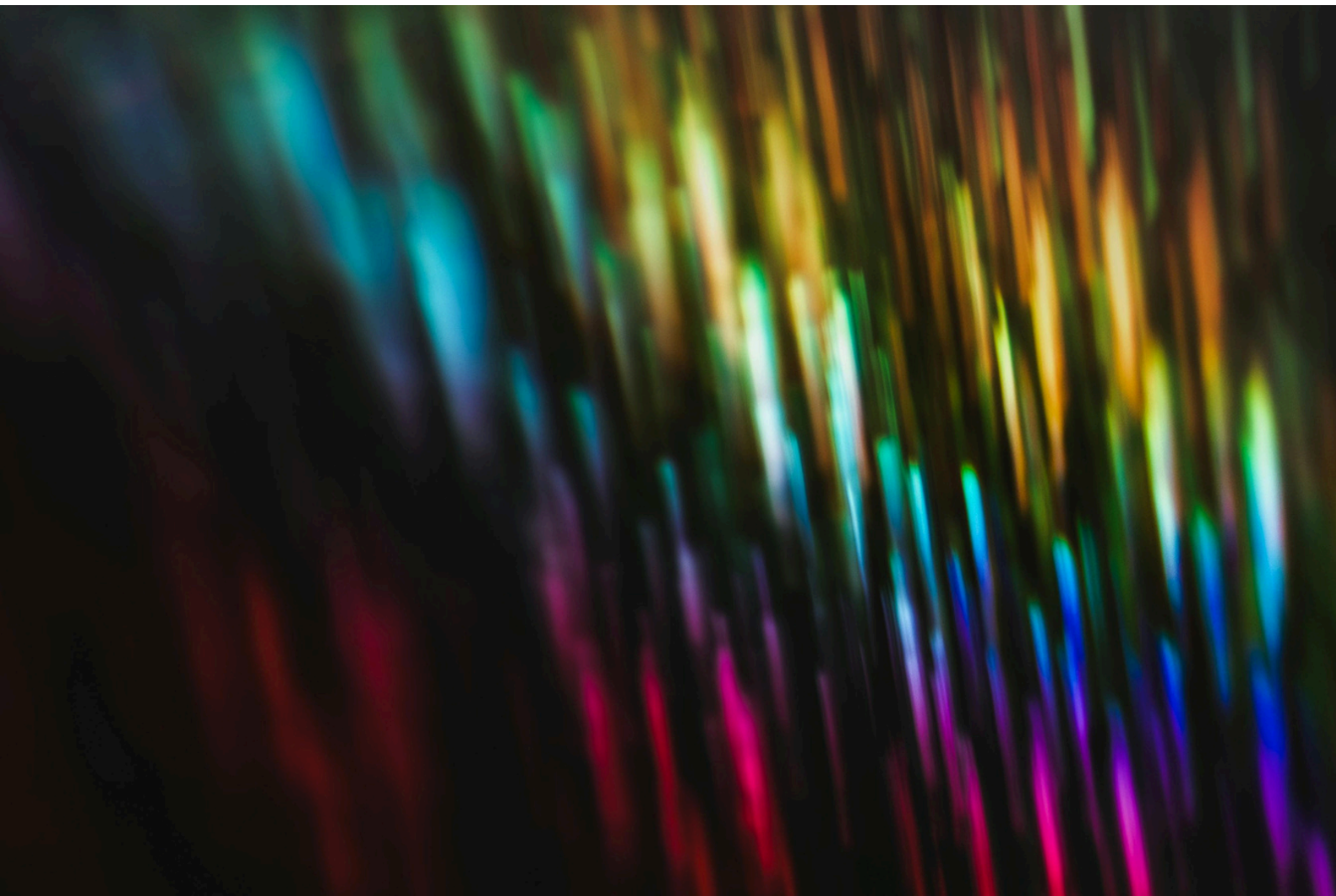
Introducción

Disponer de comunicaciones cifradas es esencial para coordinar operaciones críticas en tiempo real. Las comunicaciones tácticas son un pilar fundamental en el ámbito de la defensa, ya que permiten la ejecución segura y efectiva de misiones sensibles y de alta complejidad. Sin embargo, las comunicaciones tácticas no se limitan al ámbito militar; también son vitales para infraestructuras críticas como los sectores energéticos, transporte, seguridad ciudadana, protección civil y servicios de emergencia, entre otros.

La creciente digitalización ha expuesto estas redes a nuevos riesgos. Según un informe de **Eurelectric** publicado en noviembre de 2024**,** los ciberataques en el sector energético europeo se duplicaron entre 2020 y 2022, registrándose 48 ataques públicos conocidos, de los cuales 15 afectaron directamente los sistemas operativos de redes eléctricas. (smartgridsinfo.es)

Además, se ha observado un **aumento de ataques dirigidos contra organismos estratégicos**, como cuerpos policiales y centros de control de emergencias, con el objetivo de interferir en la capacidad de respuesta ante situaciones críticas.

En este contexto, **securizar las comunicaciones tácticas** ha dejado de ser una opción técnica para convertirse en un imperativo estratégico que **garantiza la eficacia y continuidad operativa, la protección de vidas y la soberanía tecnológica nacional**.



Estado actual de las comunicaciones cifradas

Las organizaciones que gestionan infraestructuras críticas o prestan servicios esenciales suelen implementar diversas medidas para securizar sus comunicaciones tácticas:

Cifradores independientes
Los cifradores, **dispositivos o programas que encriptan la información**, se utilizan de forma generalizada para proteger datos en tránsito. Sin embargo, si se usan de forma aislada, pueden surgir problemas de gestión y escalabilidad. Por eso, es vital que los cifradores se integren plenamente en sistemas de seguridad con múltiples elementos coordinados que permitan una respuesta eficaz y confiable.

Las claves
La seguridad de un sistema de cifrado depende en gran medida de una **gestión adecuada de las claves criptográficas**. Esto **requiere un sistema centralizado y seguro para la generación, almacenamiento y distribución** de estas claves, siendo la única forma de mitigar los riesgos de exposición y proteger nuestras comunicaciones cifradas.

Medios de transferencia

Otro reto para las organizaciones es **contar con mecanismos seguros para la transferencia de claves** desde el sistema de gestión hasta los cifradores, sin abrir brechas de seguridad que comprometan nuestras comunicaciones. Actualmente, evitamos estas brechas retirando dispositivos obsoletos y protocolos que no cumplen con los últimos requisitos de seguridad, para evitar que nuestras claves sean interceptadas o manipuladas.

Implementación de criptosistemas integrales

Para adoptar un enfoque holístico en la securización de nuestras comunicaciones tácticas, proponemos la **creación de criptosistemas integrales que aseguren una protección completa de todas las comunicaciones cifradas**. Los diferentes componentes que conforman nuestro criptosistema deben estar debidamente interconectados para trabajar de manera armoniosa, garantizando la seguridad de la información en todo momento.

Un criptosistema no es, por tanto, un simple dispositivo de cifrado independiente trabajando por su cuenta; es un **ecosistema global con una arquitectura de seguridad compuesta por tecnologías, procedimientos y políticas que trabajan conjuntamente para proteger las comunicaciones cifradas en escenarios operativos que requieren un alto nivel de exigencia**. La ventaja clave de un criptosistema integral es su capacidad para adaptarse a distintos entornos (militares, civiles, industriales) así como a diferentes plataformas (naval, terrestre, aérea) sin comprometer ni la seguridad ni la interoperabilidad.

Componentes esenciales de un criptosistema

Cifrador

Los cifradores que conforman un criptosistema deben ser **capaces de operar en múltiples plataformas y adaptarse a diversos entornos**, garantizando la protección de la información sin importar el medio de transmisión. Estos dispositivos **deben contar con certificaciones de seguridad, capacidades de actualización y configuración y resistencia a ataques físicos o lógicos**.

Sistema centralizado de gestión

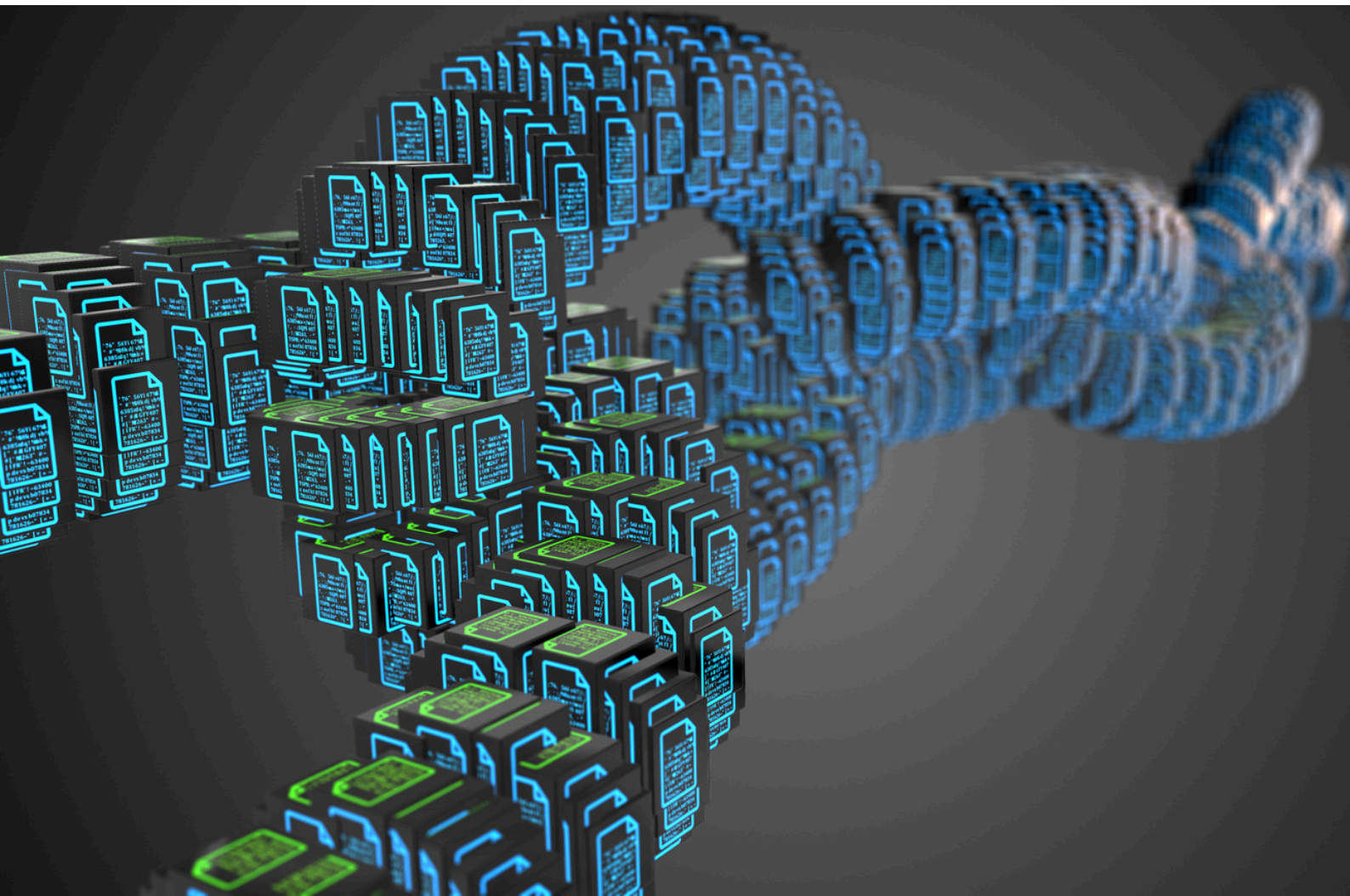
Permite la gestión y configuración de equipos de cifrado, así como la **administración eficiente y segura de las claves criptográficas**. Es crucial que este **sistema contemple políticas automatizadas de rotación y revocación de claves**, así como **registros de auditoría y control de accesos granulares** para evitar usos indebidos o filtraciones internas.

Cargador de claves seguro

La labor del cargador de claves debe ser la de un **puente confiable entre el sistema de gestión y los cifradores**. Es necesario que su diseño incluya la **capacidad de transmisión de datos bajo un interfaz de comunicación segura**, así como **mecanismos de autenticación multifacto**r para aumentar la seguridad y una gran resistencia a ataques físicos y lógicos, que permitan la protección de las claves criptográficas como elemento crítico en nuestra cadena de confianza

Además de estos tres pilares, un criptosistema debe ser **modular y escalable**, permitiendo la incorporación de nuevas funcionalidades según evolucionen las amenazas o cambien los requisitos operativos. También debe facilitar la **interoperabilidad** con sistemas aliados o de distintos organismos nacionales, sin comprometer la confidencialidad de la información.

La integración de estos sistemas **proporciona una solución robusta e integral** para proteger las comunicaciones cifradas tácticas en sectores críticos, fuerzas de seguridad, servicios de emergencia y otras entidades que requieren operar en tiempo real bajo condiciones adversas.



CERBERUS: La solución para garantizar la seguridad de la información

En respuesta a los retos actuales en materia de ciberseguridad, **Cipherbit-Grupo Oesía** ha desarrollado CERBERUS, una solución criptográfica integral diseñada y fabricada enteramente en España. Este equipo de alto rendimiento permite securizar las comunicaciones tácticas en entornos complejos y exigentes.

CERBERUS está concebido para **garantizar la confidencialidad de flujos de datos y voz en plataformas embarcadas** aéreas, navales y terrestres, a través de diferentes canales (como serie, IP o radio).

Su desarrollo, cumpliendo los requisitos más estrictos de seguridad, permite su operabilidad **tanto a nivel nacional como en el resto de los aliados de la OTAN**. De hecho, su uso ya **ha sido adoptado por el Ministerio de Defensa español,** consolidándolo como un sistema clave en la protección de infraestructuras críticas, redes militares y organismos de seguridad.

Con el lanzamiento de CERBERUS, Cipherbit-Grupo Oesía refuerza su **apuesta por el desarrollo de tecnología soberana**, orientada a fortalecer la capacidad nacional de respuesta frente a amenazas cada vez más sofisticadas.

Por

Lourdes Velasco

Directora de
Estrategia y Desarrollo de Negocio
en Cipherbit-Grupo Oesía

oesia grupo

oesia networks grupo oesia · tecnobit grupo oesia · cipherbit grupo oesia · UAV Navigation grupo oesia · inster grupo oesia

Crear un mundo mejor, más eficiente, seguro y sostenible

grupooesia.com