

TENIENTE GENERAL JOSÉ MARÍA MILLÁN, DIRECTOR GENERAL DEL CENTRO DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (CESTIC)

---

# «LA TECNOLOGÍA DEBE TENER CORAZÓN HUMANO»

Destaca que la transformación digital del Ministerio de Defensa «nos está haciendo más eficientes»

«**L**A tecnología solo sirve si tiene corazón humano», afirma el teniente general José María Millán Martínez, que el 5 de junio tomó posesión de su cargo como director general del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC). Un nombramiento con carácter de continuidad, ya que desde octubre de 2019 está al frente de este organismo, convertido el pasado mes de febrero en dirección general para responder a los retos crecientes que plantean el auge de las nuevas tecnologías y la transformación digital. «Más que un ascenso orgánico —explica este militar zaragozano de 59 años—, lo hemos entendido como un refuerzo de la confianza del equipo directivo del Ministerio en el CESTIC», formado por 249 militares y 91 civiles y dependiente de la Secretaría de Estado de Defensa y, en el ámbito operativo, del JEMAD.

«Hoy nos relacionamos, trabajamos y comerciamos en un ambiente digital,

en el que también combatimos —indica el teniente general Millán—. Lo primero que hace a diario cualquier persona del Ministerio de Defensa es encender un ordenador; lo segundo, ver su correo corporativo; lo tercero, imprimir un documento en una impresora de red...; para la actividad del Departamento y de las Fuerzas Armadas este entorno es imprescindible. Por ejemplo, no se puede entender el desarrollo de los grandes programas de obtención de sistemas de armas sin una estructura digital que lo soporte».

—¿A qué se debe esta modificación del rango del CESTIC?

—Creo que ha sido la consecuencia lógica de asumir que la información es un recurso estratégico para la defensa, tan relevante como los demás: el financiero, el de armamento y material y el capital humano, por citar algunos. Cada uno de ellos es gestionado para todo el Departamento por órganos directivos que impulsan las políticas que definen dichos recursos, y todos esos órganos

son direcciones generales. En el caso de la información, son tres las políticas departamentales que definen los objetivos y proporcionan el marco para su gestión: la de los sistemas de información y comunicaciones, la de seguridad de la información y la estrategia de la información y el conocimiento. Era una necesidad sentida hace ya tiempo adecuar el nivel del órgano directivo a tres políticas de este calibre.

—¿Qué relevancia tiene la transformación digital en el Ministerio de Defensa?

—Tiene una influencia transversal. Nos está haciendo más eficientes y eficaces, y es el elemento imprescindible para que las Fuerzas Armadas vengán en el combate multidominio. Por eso, mi visión de la transformación digital como Oficial Jefe de la Información del Ministerio se enfoca a que las Fuerzas Armadas dispongan de la espina dorsal digital necesaria para que cumplan su misión ante un adversario tecnológicamente avanzado.



de la línea de la tecnología, desde que se genera hasta que llega a su objeto. Esa cámara es altísimamente tecnológica, pero detrás hay un artista —señala, refiriéndose al fotógrafo—, y delante hay un objetivo, que es otro ser humano. Sin el ser humano no hay tecnología.

—¿Lo que está pasando ahora es nuevo?

—No, siempre ha ocurrido. Ortega y Gasset sostenía que el ser humano precisa de la técnica para adecuar la naturaleza a sus propias necesidades. Es el único animal que no se adapta al medio, sino que adapta el medio a su realidad, y lo hace a través de la tecnología. La gran diferencia es que la tecnología digital ha potenciado el poder transformador del resto de las tecnologías. Y nos ha generado, además, una nueva realidad. Ahora estamos acostumbrados a videoconferencias; antes de la pandemia no lo estábamos tanto. El siguiente paso serán los encuentros en el metaverso, ya se están desarrollando en las grandes corporaciones. Es otra realidad, pero a la que no se debe tener miedo, sino que hay que saber entenderla y aprovechar sus muchísimas ventajas. Si no la conocemos, nos ponemos en manos de los tecnólogos o de la propia tecnología.

—En su toma de posesión insistió en la importancia de los datos para cumplir los cometidos de las Fuerzas Armadas.

—Sí, el gobierno del dato es básico para que haya una verdadera transformación digital. Es una materia compleja y difícil en nuestro Ministerio, acuciado por una elevada rotación de las personas, derivada de las condiciones de la carrera militar. También lo es porque los beneficios de tener bien gobernados nuestros datos se ven a medio plazo, y los militares estamos inmersos en la urgencia...; para esto se necesita «paciencia estratégica». Solo si conseguimos gobernar nuestros datos, emplearemos seguros la inteligencia artificial.

—¿Cómo es la nueva estructura del CESTIC?

—El Centro mantiene una filosofía que está inspirada en las mejores prácticas reconocidas para organizaciones generadoras de servicios digitales. Cuenta

—¿Cuáles son los principales retos?

—El más importante es el cultural, porque la transformación digital es un proceso de cambio profundo y requiere adoptar una nueva mentalidad. Esta mentalidad se fundamenta en varios pilares: fomentar la capacidad de adaptación; conseguir la eficacia por medio del trabajo por procesos; ser conscientes de que todos somos responsables de la seguridad de la información; generar, gestionar y preservar el talento digital; y educar en la toma de decisiones basadas en datos. Estos elementos se complementan con la filosofía del mando orientado a la misión. Cuando se sincronicen esos pilares con esta filo-

sofía, estaremos en el buen camino para lograr que nuestros líderes militares se desenvuelvan en el próximo combate, que ya está siendo digital.

—¿El elemento humano perderá valor en un mundo tecnológico?

—Todo lo contrario, es más importante que nunca. Detrás de la tecnología, haciéndola funcionar, rediseñándola, segurizándola, manteniéndola, se encuentran hombres y mujeres. La tecnología se debe orientar a mejorar los resultados del trabajo de las personas; y en el Ministerio de Defensa, a que los soldados, marinos y aviadores venganzan en el combate. Hay personas en los dos extremos

### «La nueva Infraestructura Integral de la Información de la Defensa es necesaria para que el Ministerio cumpla sus cometidos»

con una División de Diseño y Evaluación de Arquitecturas; dos subdirecciones generales, la de Transformación Digital, responsable de la infraestructura y los desarrollos, y la de Planes y Servicios de Información y Telecomunicaciones, a la que compete la operación y provisión de los servicios CIS y del planeamiento del CESTIC; y una Jefatura de Ciberseguridad, con ámbito de actuación en toda la plataforma tecnológica del Ministerio. Todo ello se completa con la Oficina del Oficial Jefe de la Información y elementos de apoyo imprescindibles, como la Suboficialía Mayor y la Unidad de Gestión Económico-Financiera. Esta estructura nos permite agilizar el impulso de las tres políticas mencionadas en beneficio de las Fuerzas Armadas en operaciones y del conjunto del Departamento en sus cometidos.

—¿Qué conlleva su cargo de Oficial Jefe de la Información del Ministerio de Defensa?

—En las grandes organizaciones han proliferado los niveles C,s: el CFO, responsable de Finanzas; el CTO, de Tecnología, y el CIO (*Chief Information Officer*), de la Información. Están en el nivel más alto de la corporación e incluso reportan directamente a los comités de dirección de esas organizaciones; el CIO, en concreto, impulsa la transformación digital. Eso me permite tener una relación muy estrecha con el CIO de la OTAN y con la Agencia de Comunicaciones y de Información de la Alianza, y con la Secretaría General de Administración Digital, en el caso de la Administración General del Estado.

—¿Qué proyectos de modernización tecnológica se están impulsando?

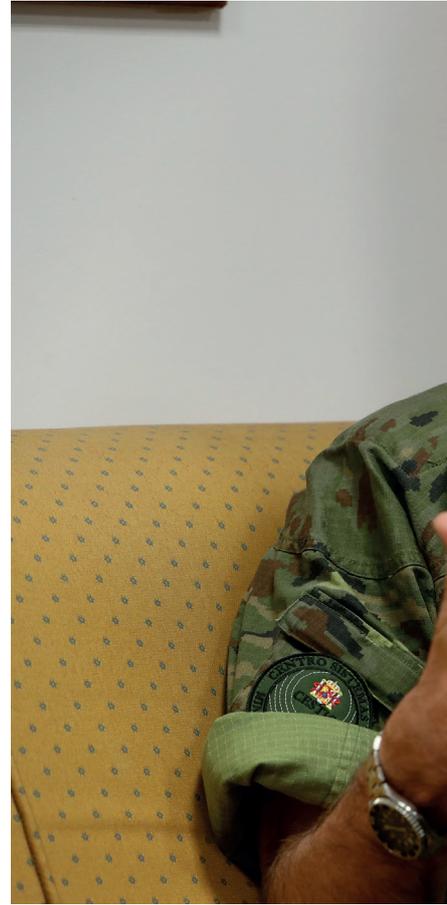
—Queremos culminar en 2023 lo que tenemos en marcha, que es muchísimo. Los proyectos más relevantes se pueden agrupar en dos grandes esfuerzos. El primero de ellos es el de completar el despliegue de la triada digital: la I3D, el Sistema de Mando y Control

Nacional y la plataforma ARGO. Este verano declararemos la capacidad operativa inicial de la I3D, la nueva Infraestructura Integral de la Información de la Defensa, porque cumple los requisitos de número de emplazamientos con el nuevo equipamiento, la gestión única, la ciberseguridad... En cuanto al Sistema de Mando y Control Nacional, nos dirigimos hacia el modelo unificado que se alcanzará a finales de 2024, cuando el sistema alcance su capacidad operativa final. Se pretende desarrollar e implantar una necesidad de las Fuerzas Armadas, que son los nodos desplegables. Respecto a la plataforma ARGO, seguiremos avanzando en el gobierno del dato y la automatización de procesos, y comenzaremos a proporcionar inteligencia de negocio, de forma que tendremos mejor información para tomar decisiones en los momentos oportunos.

El otro gran reto es culminar los grandes proyectos de renovación tecnológica, financiados por los fondos del Plan de Recuperación, Transformación y Resiliencia, procedentes de la Unión Europea. Destaca la modernización del Sistema de Personal, SIPERDEF; del Portal Personal, DICODEF; del Sistema de Mensajería, SIMENDEF; del Sistema de Aprovechamiento de Capacidades Profesionales del Personal Militar, SAPROMIL...

—¿Qué otras acciones se encuentran en marcha?

—Este año hemos sustituido el sistema de información hospitalaria del *Gómez Ulla*. Ha sido una operación delicadísima por la imprescindible necesidad de asegurar la continuidad del servicio, y en ella hemos contado con la colaboración de la Inspección General de Sanidad y de todo el personal del hospital, que dieron un ejemplo de cómo se afronta el cambio. Tenemos que terminar de estabilizar el sistema e implantar el sistema de información de imágenes. También seguiremos coordinando desde el CESTIC los proyectos de 5G y de transformación digital de los Ejércitos y la Armada.



Además, Defensa tiene en marcha más de 50 proyectos de transformación digital, todos ellos de enorme impacto en el trabajo de todos en el Departamento. Seguimos un proceso permanente de renovación tecnológica, que afecta a equipamiento de usuario y a actualizaciones de muchas aplicaciones que hacen posible el trabajo del Ministerio y de las Fuerzas Armadas.

—¿Por qué es importante la I3D?

—Porque es la espina dorsal digital del Departamento. A ella se conectarán los centros de decisión de todos los niveles —político, estratégico, operacional y táctico—, los emplazamientos de la Defensa —los más críticos conforman lo que conocemos como Núcleo Protegido— y las unidades en zonas de operaciones. Centros de decisión, emplazamientos, unidades y usuarios acceden a los servicios digitales que la I3D proporciona: telefonía segura, motores de automatización de procesos, inteligencia artificial, herramientas de ciberseguridad, servicios de movilidad, teletrabajo...

La I3D aporta servicios digitales clasificados, para el mando y control y la gestión de la información clasificada,



y no clasificados, para la gestión corporativa del Departamento. Gracias a ella accederemos a las infraestructuras tecnológicas de la OTAN y la UE, y a las de la Administración General del Estado. Sin la I3D es imposible que el Ministerio —es decir, las Fuerzas Armadas, los órganos directivos, las unidades desplegadas en operaciones, los grandes programas de armamento y material...— desarrolle sus cometidos. Es uno de los principales habilitadores de las misiones militares.

—Desde el punto de vista de las comunicaciones, ¿qué estamos aprendiendo de la guerra en Ucrania?

—Lo resumiría en una palabra: agilidad. La tecnología proporciona una nueva agilidad en el entorno operativo moderno. En la segunda guerra mundial, el más grande venció al pequeño. En la guerra fría, el rápido pudo con el lento. Ahora se trata de ser ágiles, adaptativos, abiertos a un entorno cuya apariencia no deja de sorprendernos, porque nunca es como esperábamos. La propia tecnología está proporcionando servicios digitales enfocados a la misión, adaptados a la realidad del usuario y respondiendo fielmente a lo que se re-

quiere en el campo de batalla. Son soluciones posibles, orientadas a cumplir los cometidos, y se emplean estrictamente para lo que se necesitan. Esto también es una lección identificada: tenemos que aprender a levantar requisitos de las aplicaciones que necesitamos, dominar nuestro nivel de ambición y definir claramente la finalidad de la herramienta que esperamos.

—¿Qué tecnologías marcarán el futuro del campo de batalla?

—Es difícil predecirlo con exactitud. Estos últimos años nos han enseñado a ser más cautos en ejercicios de prospectiva..., pero hay elementos decisivos que encontraremos con casi total segu-

**«El uso militar de la inteligencia artificial debe estar presidido por un código ético que refleje los valores morales»**

ridad en el entorno operativo futuro y que nos permitirán intuir las tecnologías que necesitaremos; así, el entorno será inteligente, interconectado, digital y distribuido. Creo que la computación cuántica marcará el punto de ruptura de ese entorno y que su integración con las demás tecnologías —aumento de la capacidad de computación, la tecnología de nube, 5G...— pondrán a disposición del combatiente lo que requiere para vencer en el próximo combate.

—¿Podremos confiar en la inteligencia artificial?

—Es difícil limitar una tecnología como la inteligencia artificial. Seguramente sea complejo y más ahora mismo imaginar qué límites serán los necesarios. El uso militar de esta potentísima tecnología debe estar presidido por un código ético que refleje los valores morales que siempre han definido al individuo en el combate y han humanizado todo lo posible el drama de la guerra.

—¿La ciberseguridad sigue siendo la gran asignatura pendiente?

—Es una asignatura de la que nos examinamos todos los días, pero no por hacer mal nuestros deberes. El Ministerio de Defensa es muy consciente de que la ciberseguridad es parte inseparable de la transformación digital y la ha incluido en la visión del CIO de este proceso de cambio. La ciberseguridad es responsabilidad de todos, porque cada uno de nosotros empleamos el ciberespacio para desarrollar los cometidos de cada puesto de combate. Es fundamental aumentar la conciencia de seguridad en el ciberespacio. El CES-TIC incorpora la ciberseguridad desde el diseño de los nuevos servicios.

—¿Entendemos la necesidad de estos cambios?

—Lo digital es una realidad de la que no podemos huir. No advierto resistencia al cambio; solo diferentes velocidades y niveles de ambición en los distintos ámbitos del Ministerio, que se topan con la necesidad de armonizarlo todo desde esta nueva dirección general. Hemos avanzado notable y notoriamente. Queda mucho por hacer, sin duda, pero mucho menos que antes.

Santiago F. del Vado  
Fotos: Pepe Díaz