

# APRENDER A COMBATIR EN EL CIBERESPACIO

La nueva Escuela Militar de Ciberoperaciones instruye al personal de las FAS para detectar y hacer frente a los ataques en las redes informáticas



Alumnos del primer Curso Básico de Especialización en Ciberoperaciones durante una de las clases.

**L**AS amenazas en el ciberespacio son cada vez más sofisticadas, profesionales y peligrosas, y ningún organismo público o privado está libre de sufrir estos ciberataques. Las Fuerzas Armadas tampoco. Por ello, necesitan disponer de las capacidades necesarias para hacerles frente de manera rápida y efectiva, y, lo principal, es que su personal cuente con la formación adecuada.

Con este objetivo se ha puesto en marcha la Escuela Militar de Ciberoperaciones, un centro que aún está dando sus primeros pasos. «Nuestra idea es que todo el que ingresa en las Fuerzas Armadas y se quiera dedicar a la ciberdefensa, lo primero que haga sea el Curso Básico de Especialización en Ciberoperaciones», señala el director de la Escuela, coronel Francisco Palomo Pérez. Pero reconoce que están empezando. «No tenemos todo

el personal y los medios que necesitamos. Todavía podemos mejorar mucho».

Creada en febrero de 2023 la Escuela utiliza para las clases dependencias del Mando Conjunto del Ciberespacio (MCCE), situado en la base militar de Retamares (Pozuelo de Alarcón, Madrid). «Algunos compañeros no me hablan — bromea el coronel— porque les quito las salas». Una circunstancia que quedará subsanada con la construcción de un

edificio en el mismo recinto, justo enfrente del MCCE. «Tendremos un espacio propio y diferenciado, y la formación no estará clasificada, de modo que podrán venir alumnos de otros ámbitos, sin necesidad de que cuenten con una habilitación de seguridad». Ya se han interesado por estos cursos la Guardia Civil, la Policía Nacional e, incluso, algunos países iberoamericanos.

«Esta Escuela nos da un valor añadido —puntualiza el coronel Palomo—. En el mundo civil hay mucha oferta de formación, muy buena, pero no existen estudios de planeamiento de operaciones militares en el ciberespacio. Nosotros tenemos la ventaja de que trabajamos para un único cliente, las Fuerzas Armadas, y los cursos los hacemos a su medida, preguntando a las unidades lo que necesitan».

El primer curso que impartió la Escuela fue el Básico de Ciberoperaciones en las modalidades Ofensiva, Defensiva e ISR. Finalizó el pasado 13 de octubre y lo realizaron 24 militares de tropa y marinería (16 del Ejército de Tierra, cuatro a la Armada y otros cuatro del Ejército del Aire y del Espacio). «Estamos muy contentos con el resultado —señala el director del centro—. No sabíamos cómo iba a salir la primera vez. Tuvimos la ventaja de que los alumnos tenían experiencia y conocimientos previos en ciberdefensa. Por eso, hicieron directamente las especialidades».

El primer Curso Básico de Especialización en Ciberoperaciones comenzó pocos días después con 20 soldados y marineros y, a ellos, les seguirán otros dos grupos similares, también de 20 personas, a mediados de enero y finales de febrero de 2024. Dentro de unos meses, estos 60 militares regresarán de nuevo a la Escuela para recibir una enseñanza más específica —están previstas seis especialidades— en función de las habilidades que hayan demostrado. Cuando finalicen todo el ciclo, habrán recibido 700 horas de formación. También se baraja la posibilidad de impartir un máster para oficiales y cursos de especialización para suboficiales.

Para acceder a los cursos, los soldados deben estar en posesión de una titulación de Formación Profesional de grado medio en sistemas de microinformática en red. «Pero nos gustaría que pudieran venir aquellos que tengan una titulación superior», indica el coronel Palomo. Para ello, sería imprescindible que, independientemente



El equipo de la Escuela Militar de Ciberoperaciones está formado por cinco militares, encabezados por su director, el coronel Francisco Palomo (segundo por la derecha).

mente de su titulación, se les otorgue la misma puntuación porque ahora, con una FP de grado medio, los aspirantes consiguen 30 puntos pero con una superior, tan solo 16.

«Se hace para evitar la sobrecapacitación, pero creo que si tengo a un ingeniero informático que quiere ser soldado, no pasa nada; a la larga encontrará su camino», añade. Además, una mayor formación asegura una trayectoria más larga en el mundo de la ciberdefensa. «Hay alumnos que tienen mucho interés, pero con sus conocimientos no pueden llegar muy lejos. Y necesitamos a Cristianos Ronaldos y Mesis que sean capaces de meter goles. Este es el perfil que queremos para lograr un nivel lo más alto posible», asegura el director del centro.

## Los alumnos reciben 700 horas de formación, entre la enseñanza básica y las especialidades

De los alumnos del primer de curso de Especialización en Ciberoperaciones casi ninguno tenía conocimientos sobre la materia antes de llegar a la Escuela, pero a todos les habían hablado de las posibilidades que ofrece esta especialidad, tanto dentro de las Fuerzas Armadas como en el mundo civil, así como de la oportunidad que tenían de formarse en el nuevo centro. A todos, también, les gustaría desarrollar su profesión en el Mando Conjunto del Ciberespacio. «Pasaba un tren y me he montado», señala el cabo primero Juan Luis Marín Salazar. «El mundo de la ciberdefensa avanza muy deprisa y hay que estar al día».

### ESPECIALIDADES

En la Escuela, de momento, se han puesto en marcha tres de las seis especialidades que tienen previstas: analista de SOC (Centro de Operaciones de Ciberseguridad), inteligencia en ciberamenazas y curso de ataque. El analista de SOC es el responsable de proteger y defender los sistemas informáticos. Para ello, los monitoriza y recibe todas las alertas que presentan y, cuando observa algo anómalo, es capaz de decidir si es un comportamiento habitual, si es un fallo de configuración o si se trata de alguien que está intentando acceder al sistema o que ya haya accedido.



## La Escuela pertenece al Mando Conjunto del Ciberespacio creado hace tres años en el acuartelamiento de Retamares

El especialista en inteligencia en ciberamenazas, por su parte, está pendiente de lo que hace el enemigo en el ciberespacio para, así, saber como y de quien defenderse y como atacarlo si fuera necesario. «Los especialistas en ataque hacen pruebas con nuestras propias redes para comprobar que no son vulnerables. Observan los métodos que utiliza el enemigo y los replican. Es decir, juegan con el rol de otro», explica el coronel Palomo.

El trabajo de los auditores, por su parte, es fundamental porque «todos los sistemas que tenemos montados deben pasar periódicamente una auditoria para mantener la acreditación de seguridad», explica el director de la Escuela.

La tercera, implantador de sistemas, será la última especialidad que se incorpore a la oferta de estudios del centro.

Actualmente, en la Escuela Militar de Ciberoperaciones están destinados cin-

co personas son muy pocas para sacar adelante todo lo que demanda la Escuela. «Aunque los profesores son muy buenos, queremos dar nuestro barniz militar a las enseñanzas y eso solo lo podemos hacer los propios militares». Su objetivo es que cuando empiece a aumentar la plantilla del Mando Conjunto del Ciberespacio, ese incremento se vea reflejado también en la plantilla de la Escuela.

En el MCCE, actualmente, están destinadas 400 personas entre civiles y militares. El objetivo es que, antes de finales de 2028, sean unos 1.200 militares y unos 300 civiles, aún muy por debajo de países como Francia, que en el año 2025 dispondrá de 5.500 personas dedicadas a estas tareas.

Para el coronel Palomo, el problema de esta falta de profesionales reside en que los Ejércitos se resisten a perder efectivos que necesitan para sus unidades terrestres, navales o aéreas. «No es que no sean conscientes de la importancia de este campo; es un problema de números, de plantilla».

Por otra parte, cada vez resulta más difícil retener al personal especializado, porque el mundo del ciberespacio está muy cotizado en la calle. «Por eso tenemos que ofrecerles algo que sea atractivo para que se queden, necesitamos conseguir una masa crítica de personal, y que haya repuestos para los que se van».

De cara al futuro, el coronel Palomo destaca también la necesidad de disponer de un campo de maniobras virtual «con escenarios ya preparados que nos permitan realizar simulaciones». Aunque reconoce que en los últimos años se han dado pasos muy decididos e importantes el director de este nuevo centro docente piensa que queda mucho por hacer. «En esto del ciberespacio todo el mundo va corriendo y si lo haces a una velocidad más lenta que los demás, te vas quedando atrás. Tampoco hay que inventar nada, solo ver lo que están haciendo los países de nuestro entorno», concluye.

**Elena Tarilonte**  
**Fotos: Hélène Gicquel**



Las clases se imparten de manera provisional en dependencias del Mando Conjunto del Ciberespacio, a la espera de que se construya un edificio independiente en el mismo recinto de la base Retamares.

Para instruirse, también trabajan habitualmente con empresas. «Es un beneficio recíproco; les hacemos un estudio desde el punto de vista del atacante, les decimos las vulnerabilidades que tienen. Nosotros nos instruimos y las empresas mejoran su seguridad», añade.

Las otras tres especialidades que se impartirán en la Escuela son las de investigador digital, de auditoría de sistemas y de implantador de sistemas. Los primeros se dedican a observar lo que ha pasado en otros sitios y buscan pruebas —amenazas— de ello en sus propios sistemas.

co militares y para las tareas docentes se contratan profesores externos. Los que impartieron el primer curso pertenecían a la Universidad de Vigo y las clases fueron *online*. «Pero ese no es nuestro modelo; entendemos que la formación debe ser presencial», señala el coronel. Por eso, ahora los docentes los proporciona una empresa, excepto los que imparten la asignatura de ciberdefensa, que son militares. «Les damos unos conocimientos básicos sobre la estructura de la defensa nacional y de los Ejércitos, para que se familiaricen con este mundo».