TEMAS PROFESIONALES

LA GESTIÓN DE LA SEGURIDAD EN LAS GRANDES INSTALACIONES

Samuel MORALES MORALES

N gran número de los emplazamientos de la Armada pueden ser considerados grandes instalaciones, destacando por encima de todas ellas la Base Naval de Rota, en cuyo interior, además de otros centros críticos, se incluyen un puerto y un aeropuerto. La gestión de la seguridad física en ellas representa un verdadero reto de gestión e integración de sistemas, no suficientemente resuelto hasta la fecha.

Estas instalaciones se caracterizan por perímetros extensos, en algunos casos con zonas que tienen un carácter histórico y que deben ser tratadas de forma específica; se sitúan dentro de núcleos urbanos o

Base Naval de Rota. (Foto: *www.flickr.com/photos/armadamde*)

fuera de ellos; en la mayor parte de las ocasiones incluyen un frontal marítimo y normalmente albergan varias unidades, no siempre dentro de la misma cadena orgánica, conformando lo que se conoce como un entorno compartido de seguridad.

Además, en nuestros arsenales y bases navales es norma común el libre movimiento por la mayor parte de las instalaciones una vez superado el control de acceso que, según recogen algunas normas interiores, también se concede a personal externo a la organización, aunque este debe ir acompañado durante la visita, que puede realizarse a cualquier hora del día y de la noche sin ningún tipo de restricción.

Esta libertad de movimiento hunde sus causas en aspectos tan dispares como la existencia de instalaciones deportivas en el interior del recinto militar que pueden ser utilizadas fuera de horario laboral por personal civil; los clubes o mesones en los que se organizan actividades lúdicas; la autorización de actividades de pesca desde los muelles de la instalación para mantener la relación con el entorno, o simplemente para visitar desde el exterior los buques y unidades. Además, en los últimos años se ha sumado, aunque de momento de forma no generalizada, el vuelo de vehículos aéreos no tripulados de propiedad privada en el interior de las instalaciones por personal militar.

Todas estas circunstancias y costumbres plantean un verdadero reto a la seguridad física, máxime en el nivel de alerta antiterrorista que desde junio de 2015 fue establecido como alto por el Ministerio del Interior en todo el territorio

nacional. Reto que al ser gestionado no puede obviar la tradicional y necesaria vinculación de las familias del personal militar con las unidades y que afianzan unas relaciones que van mucho más allá de las meras profesionales.

Resulta evidente que nos encontramos ante la gestión de una situación que requiere múltiples equilibrios. Equilibrio entre la protección de los bienes críticos que existen dentro de la base y el desarrollo de actividades más allá de las meramente profesionales; también entre la seguridad deseable en toda la instalación y la necesaria en sus elementos críticos; entre el recurso económico imprescindible y el disponible, así como entre los diferentes sistemas de seguridad existentes en el interior de esas grandes instalaciones, y finalmente, entre la entidad del recurso humano especialista en seguridad y los cometidos asignados.

Breve aproximación a la gestión de la seguridad física en grandes instalaciones

En el análisis de las necesidades de seguridad que se plantean en un escenario de la complejidad de una gran superficie, podemos encontrar cierto paralelismo con los requerimientos que, en este ámbito, se suscitan en una gran ciudad. En cierto modo, intuimos un contexto equiparable en muchos aspectos debido a la multiplicidad de necesidades coincidentes que hay que atender.

Nos enfrentamos a una especie de ciudad a escala en la que tenemos que proteger los elementos críticos y también las personas, teniendo en cuenta además las exigencias y los riesgos añadidos que entraña gestionar la seguridad de un lugar por el que transitan diariamente cientos de personas, ya sean las destinadas en la propia instalación, personal civil contratado por alguna de las empresas que presta servicios en ella o proveedores, permanentes o temporales, que acceden al recinto con cierta frecuencia.

En este tipo de instalaciones, más que nunca, es imprescindible un desarrollo integrador de la seguridad electrónica, con una visión centralizada, capaz de gestionar eficaz y simultáneamente muchos puntos distintos y también distantes, afectados a su vez por parámetros variables. El enorme volumen de información que recogen estos sistemas de seguridad debe confluir de manera simplificada en un centro de control para poder ser utilizado de forma sencilla por los operadores, que disponen así de unas herramientas eficaces para el desempeño de su trabajo. Desde esta sala de control, las instalaciones son supervisadas de manera permanente e inteligente las 24 horas del día, dando cobertura no solo al horario laboral, sino también a todas las actividades que se desarrollan fuera de este. Los sistemas integrados de circuito cerrado de televisión (CCTV) deben abarcar el perímetro y las instalaciones críticas, pero también los accesos exteriores e interiores, los depósitos de material sensible, las áreas de carga y descarga y los estacionamientos.

Una gran superficie es un lugar en el que es necesario prever la distribución estratégica de centenares de cámaras y cubrir la seguridad de miles de puntos de intrusión. La eficacia de la tecnología en estos casos exige el funcionamiento coordinado y óptimo de automatismos que trasladan al centro de control toda la información necesaria para que el factor humano, los operadores y el personal de guardia dispongan de los datos necesarios para actuar de manera eficiente y en tiempos de respuesta óptimos.

Uno de los aspectos de mayor relevancia, como ya hemos adelantado en la introducción, es que la implantación de los sistemas tecnológicos debe convivir en armonía con el desarrollo de las actividades profesionales y no profesionales que se desarrollan en el interior de las instalaciones navales. Es imprescindible conjugar adecuadamente la protección de las instalaciones críticas con la circulación del personal por las mismas. En caso de alarma, deben desencadenarse respuestas protocolizadas dependiendo del nivel de riesgo al que se enfrenta la gestión de la seguridad.

Esta rápida aproximación a la seguridad de una gran superficie da una idea de la multiplicidad de riesgos que se afrontan. También permite entrever el amplio despliegue tecnológico que se precisa para dar la respuesta adecuada a cada una de las necesidades específicas que plantea cada zona:

— Perímetro y accesos externos.
— Estacionamientos.
— Zonas subterráneas.
— Puertas de acceso a instalaciones críticas, zonas de acceso restringido o depósitos de material sensible.
— Zonas de ocio y restauración.
— Muelles de carga y descarga para proveedores.

Además, se deben gestionar de forma eficiente aspectos de la vida diaria, tales como:

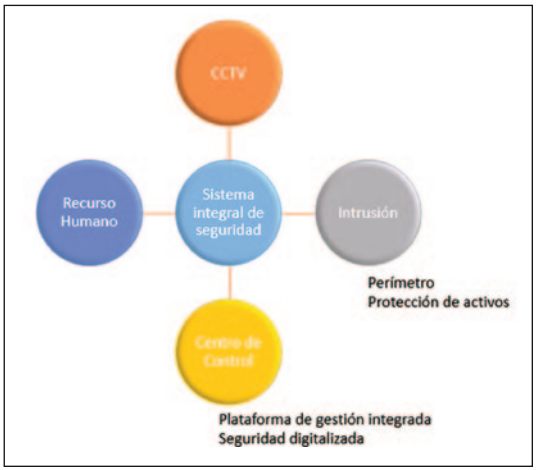
— Limpieza de zonas comunes o restringidas.
— Recogida y reciclaje diario de basuras.
— Apertura y cierre de puertas.
— Distribución y recogida de correo y paquetería.
— Encendido y apagado de luces.
— Control de accesos o de entrada y salida de vehículos.
— Orientación a las visitas y operarios de mantenimiento y/o servicios.
— Rondas periódicas de inspección, para comprobar el buen funcionamiento de las instalaciones o equipos.
— Mantenimiento de la iluminación y de los equipos electrónicos o mecánicos.

Patrulla de seguridad en puerto. (Foto: Armada)

El plan de seguridad de una gran superficie debe, por tanto, contemplar la implantación de sistemas de seguridad electrónica de muy diversas características que funcionen de manera automática e inteligente y que se constituyan en el apoyo imprescindible del personal encargado de la seguridad para abarcar la gran envergadura de aspectos a controlar y supervisar en estas instalaciones.

Los elementos fundamentales de la seguridad en grandes instalaciones

Tal como se infiere de la lectura del epígrafe anterior, la gestión de la seguridad física de las grandes superficies se sustenta en cuatro elementos fundamentales. El primero es un sistema antiintrusión que pasa, de forma inexcusable, por una clara definición de los activos críticos a proteger en los que este sistema deberá combinar la eficacia y el mantenimiento adecuados para evitar o retrasar el acceso de personas no autorizadas. La correcta determinación de los activos críticos a proteger permitirá establecer en otras zonas un perímetro con un carácter más disuasorio al que no se le exija la misma eficacia que al que rodea las instalaciones críticas. La vulneración del perímetro de una gran instalación no siempre tiene que significar un gran riesgo. Lo que sí representa un riesgo difícil de gestionar es no ser capaz de detectar esa intrusión o, una vez producida,



Elementos fundamentales de la seguridad en grandes instalaciones

no tener los medios adecuados para su neutralización o los sistemas precisos para evitar que alcance elementos críticos.

El segundo elemento es un CCTV que cubra la mayor parte de la instalación, incluida la vertiente marítima, y que proporcione alerta temprana de las posibles intrusiones o actividades delincuenciales. Este CCTV debe integrar todos los sistemas de videovigilancia existentes en las distintas instalaciones, especialmente en aquellas que puedan depender de cadenas orgánicas diferentes. La integración de todos los medios podría proporcionar, en algunas ocasiones, una vigilancia sobre las dársenas y el flanco marítimo con los elementos optrónicos de los buques, que en un gran número de ocasiones son meros elementos pasivos de la seguridad. Además, en las grandes superficies, este CCTV puede complementarse con sistemas de vigilancia instalados en drones cautivos que proporcionen un alcance mayor y permanente en un gran margen de condiciones meteorológicas.

El tercer elemento es un centro de control unificado de todos los sistemas de seguridad, equipado no solo de medios de recepción de imágenes, sino también de alarmas conectadas a sensores y, cada vez más, de un mayor empleo de la inteligencia artificial para prevenir posibles situaciones que vulneren la seguridad física. El proceso de transformación digital también debe incluir, de forma inexcusable, la gestión de la seguridad física. Esta digitalización facilitará la gestión y el control de los miles de sensores y cámaras que puedan estar instalados en una gran superficie y también el acceso diario del personal mediante el reconocimiento facial o controlar la presencia del personal en zonas no autorizadas mediante tarjetas de visita o de identificación inteligentes. En la Armada, esta integración se ha realizado de forma incipiente en el Población Militar de San Carlos. Pero, tras muchos años de dilaciones, es necesario afrontar este proyecto de forma decisiva para mejorar la seguridad física de nuestras instalaciones.

Finalmente, el cuarto elemento es el recurso humano, que podemos catalogar en tres categorías. La primera, el personal que presta servicios en los centros de control. Desafortunadamente, no es extraño encontrar centros de control supervisados por escaso personal, al que se exige una atención imposible de mantener. Este, junto con la ausencia de alarmas conectadas a sensores, es uno de los

errores más comunes que se aprecian en nuestras instalaciones. Hay que tener en cuenta que la inclusión de medios tecnológicos en la gestión de la seguridad física reduce la necesidad de recursos humanos en algunos cometidos, pero no llega a su completa eliminación y en algunos de ellos los requerimientos son exactamente iguales.

La segunda categoría estaría formada por el personal con cometidos de seguridad en los accesos o en las patrullas de seguridad. Dado su limitado número y la necesaria atención que deben mantener en todo momento, no deberían realizar tareas administrativas de gestión de autorizaciones de acceso o similares que no requieren de la necesaria especialización que proporcionan y que solo se convierten en distractores de la atención.

La tercera, y no menos importante categoría, la conforma la totalidad de la dotación de una unidad, consciente de que en sus pequeñas acciones en el día a día, desde que ingresan en la instalación hasta que la abandonan, contribuyen a la seguridad física. Innumerables son los casos de personal de las dotaciones de las unidades que no registran el acceso a una llave, que no cierran el acceso al destino al final de la jornada o que dificultan con su actitud el trabajo de los especialistas en seguridad. La seguridad física es compatible con cierto nivel de comodidad, siempre que entendamos que la seguridad es cosa de todos.

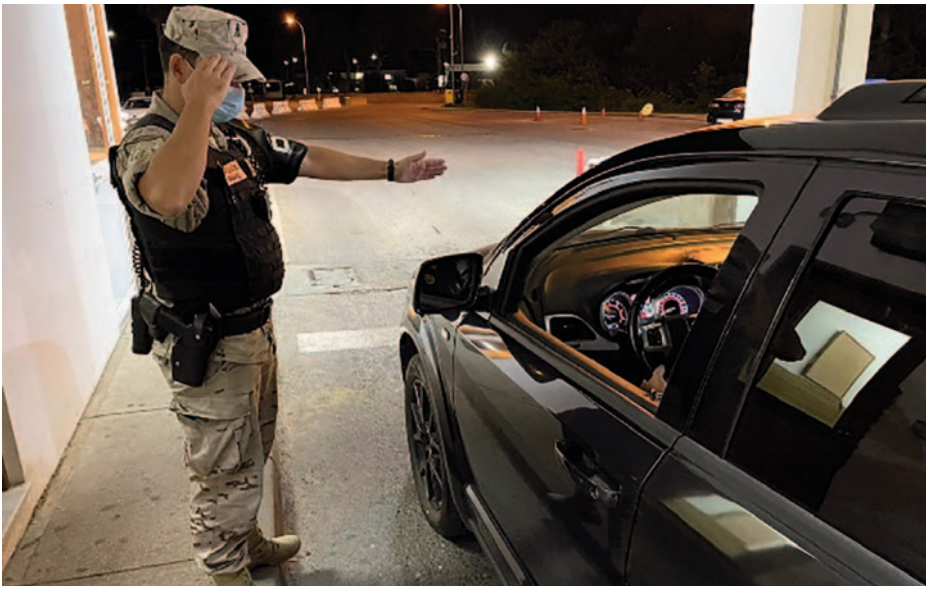
Las amenazas emergentes a la seguridad física

El exponencial desarrollo de las nuevas tecnologías ha contribuido a la mejora de nuestras sociedades. Sin embargo, su empleo malicioso, especialmente de los vehículos tripulados remotamente, plantea un reto a la gestión del potencial riesgo que estas nuevas amenazas pueden significar para las instalaciones de la Armada.

Esta gestión tiene dos ámbitos muy diferenciados y con soluciones que no son comunes. Por una parte, la amenaza que suponen los vehículos tripulados remotamente en situación de conflicto puede ser gestionada, una vez localizados, mediante la utilización de sistemas cinéticos o de energía dirigida, creando zonas de exclusión alrededor de objetivos críticos para facilitar su detección. Es un tipo de gestión a la que no nos referimos en este artículo.

El reto al que hacemos referencia es la utilización de vehículos tripulados remotamente o incluso autónomos que pueden ser adquiridos en el mercado civil y que con modificaciones menores se convierten en un auténtico riesgo para la seguridad física. Esta manipulación a la que hacemos referencia es la que está sucediendo en estos momentos en el conflicto entre Ucrania y Rusia, que convierte en inservibles muchos de los actuales sistemas contradrones.

El conocimiento sobre cómo realizar la manipulación para que un vehículo pilotado remotamente pueda sortear la mayoría de las medidas existentes ya está disponible en la red de redes, pero es de esperar que con la finalización del



Control de acceso a la Base Naval de Rota. (Foto: Fuerza de Protección de la Armada)

conflicto anteriormente referido se produzca una expansión de este conocimiento hacia ámbitos delincuenciales y terroristas, que podrán emplear estos dispositivos con fines propagandísticos, de recopilación de información o para realizar acciones de sabotaje o neutralización de elementos críticos.

¿Y entonces, qué podemos hacer?

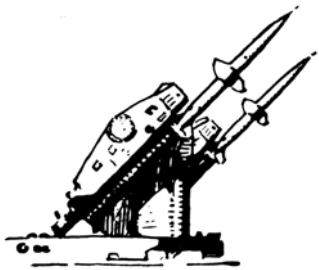
Como hemos indicado, la seguridad es compatible con cierto grado de comodidad, Además, debe ser un elemento que esté imbuido en el más profundo ADN de la cultura institucional, concienciando a todo el personal de la Armada de que la seguridad es cosa de todos. Pero también es necesario pasar de las musas al teatro y, además de la concienciación, establecer medidas que contribuyan a la gestión de la seguridad.

En primer lugar se hace indispensable definir en cada una de ellas qué elementos son críticos. Una vez definidos, se debe garantizar en ellos la eficacia de las medidas de prevención, disuasión y respuesta, evitando, además, el acceso de personal no autorizado no solo a su interior, sino también a sus inmediaciones, en horario laboral y fuera de él. Esta medida no exime de mantener un perímetro alrededor de toda la instalación, pero que puede tener un carácter disuasorio y por lo tanto implicar un menor coste.

En segundo lugar, es necesario disponer de la tecnología adecuada para detectar la intrusión y el movimiento no autorizado en el interior de una instalación, manteniendo la capacidad de reaccionar con elementos humanos. Para ello son imprescindibles la integración de todos los sistemas de seguridad y la inclusión de la digitalización de la seguridad en ellos. Un proceso ya en marcha en el mundo civil y del que no debemos quedarnos descolgados, integrando en los futuros centros de recepción de alarmas unificados (CRAU) sistemas de digitalización y análisis de la seguridad.

Finalmente, se deben tomar medidas en relación al acceso del personal a las instalaciones navales, que debe ceñirse a la «necesidad de acceder», evitando la entrada bajo una norma 24/7 incluso al personal militar destinado en la unidad; o el acceso indiscriminado a toda la instalación del personal civil, familiares e invitados. Este control se puede conseguir, de forma eficiente, con tarjetas de visita inteligentes que proporcionan trazabilidad de la posición del portador en todo momento.

Estas simples medidas, junto con la necesaria concienciación y contribución de todo el personal de la Armada, redundarán en una mejor gestión de la seguridad física de las grandes instalaciones. La mejor protección se alcanza con una adecuada combinación de medidas de concienciación, organizativas y de procedimientos y técnicas.



Submarino *Tramontana* regresando a la base y corbeta saudí *Al-Jubail* realizando calibración magnética, julio de 2022. (Foto: Antonio Arévalo Díaz del Río)