

BOLETÍN R@S

UNIDAD CENTRAL DE SEGURIDAD PRIVADA



SISTEMAS ANTIDRÓN

Páginas 1, y 14

DENUNCIAS "IN SITU"

Página 2

AVISOS EN CIBERSEGURIDAD

Páginas 3 y 4

RED AZUL: POLICÍA ESPAÑOLA EN AMERIPOL

Página 5

ENTREVISTA DETCAMP DETECTIVES 4.0

Página 6

HACKEO DE LLAVES POR PATRONES DE SONIDO

Página 7

DRONES: GRUPO PERSEO

Páginas 8 y 9

CCTV EN COMUNIDADES DE VECINOS

Página 10

LA VERIFICACIÓN PERSONAL DE ALARMAS

Páginas 11, 12 y 13

NOTICIAS

Páginas 14,15 y 16



POLICÍA NACIONAL: La POLICÍA DEL AIRE evalúa los sistemas antidrón en el Aeropuerto de Asturias.



Ver apartado noticias (página 14 y video que se adjunta)

DENUNCIAS “IN SITU”

Próxima puesta en funcionamiento

El 14 de septiembre, el Ministerio del Interior hacía pública la próxima puesta en funcionamiento del protocolo de denuncias “in situ”, con apoyo telemático, para determinados delitos leves.

Con dicho protocolo se pretende simplificar la actuación en relación con infracciones penales de menor entidad, buscando establecer los mecanismos policiales que agilicen el proceso de recepción, tramitación de denuncias y citación de determinados delitos leves, consiguiendo con ello un beneficio tanto de la ciudadanía como de la Administración.

El objeto del protocolo es establecer un procedimiento que permita de forma telemática presentar denuncias ante los agentes de las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE) por la comisión de determinados delitos leves en establecimientos comerciales, sin necesidad de que sus responsables, empleados o personal de seguridad privada deban desplazarse hasta las dependencias policiales para presentarlas.

El protocolo, inicialmente, está limitado a aquellos establecimientos que reúnen determinados requisitos en materia de seguridad privada, no excluyéndose la posibilidad de que en un futuro se pueda aplicar a otros entornos.

Asimismo, y con la misma visión de poder abrirse a otros ámbitos, en principio, se aplicará a delitos leves contra el patrimonio siempre que los autores o cómplices hayan sido sorprendidos “in fraganti” y se encuentren a disposición policial en el establecimiento comercial.

Resumidamente, los requisitos que deberán cumplir las entidades comerciales interesadas son:

- 1.- Disponer de un departamento de seguridad formalmente constituido según lo dispuesto en el Reglamento de Seguridad Privada.
- 2.- Tener contratado un servicio de vigilantes de seguridad privada que incluya la prestación específica del mismo en los establecimientos comerciales donde se pretenda tramitar denuncias “in situ”.
3. Cumplir las condiciones logísticas necesarias para garantizar, tanto la correcta conectividad a los entornos web de las FFCCSE, como disponer de un lugar con privacidad suficiente para llevar a cabo los trámites.
4. Suscribir por persona con capacidad de representación suficiente para obligarse en su nombre, un documento de adhesión con la Policía Nacional, con la Guardia Civil o separadamente con ambos, surtiendo efectos a partir de la firma por ambas partes.
5. Con carácter previo a la suscripción del documento de adhesión, las FFCCSE comprobarán que cumple el establecimiento con las condiciones de conectividad y privacidad mencionadas, así como que la entidad comercial dispone de una certificación, emitida por Seguridad Privada de la Policía Nacional, justificativa de que se dispone de departamento de seguridad y servicio de vigilantes de seguridad.

Si el servicio de seguridad tuviera carácter estacional, por campañas o con horario parcial, el protocolo solo será aplicable durante dicho periodo temporal y así se especificará en el documento de adhesión. También constará cuando, excepcionalmente, las FFCCSE dispongan la aplicación del protocolo aunque se incumpla el requisito de disponer de dicho servicio de seguridad.

Próximamente, la Policía Nacional difundirá las instrucciones concretas para la efectiva implantación del protocolo.



La Unidad Central de Seguridad Privada, ante el aumento de la ciberdelincuencia detectado durante el pasado estado de alarma y queriendo dar continuidad a la acción de información preventiva iniciada durante ese periodo, periódicamente facilita al sector de la seguridad privada los avisos de seguridad informática que publica el Instituto Nacional de Ciberseguridad.

A modo de resumen y sirviendo de recordatorio, se enumeran los últimos avisos publicados por el INCIBE:

- En los últimos días se ha detectado una campaña activa de envío de correos electrónicos fraudulentos de phishing (suplantación de identidad) dirigidos al **Banco Santander**. Los correos contienen el asunto: **«Activar la nueva seguridad gratis lo antes posible...»**. En el mensaje se indica al usuario que es necesario actualizar su cuenta bancaria para mejorar la seguridad, para ello conducen a un enlace en el que completar el proceso para reforzar las medidas de seguridad.
 - Campaña de envío de correos electrónicos fraudulentos de tipo *phishing* que trataban de suplantar a la entidad financiera **Bankia**. En la campaña identificada, el correo tiene como asunto: **«notificarte un nuevo mensaje»**. En el cuerpo del mensaje se indica al usuario que se ha realizado una actualización de la cuenta y que debe finalizar la solicitud para darle de alta las nuevas mejoras en materia de seguridad.
 - Campaña de envío de correos electrónicos fraudulentos que intentaban hacerse pasar por la entidad financiera **Banca March** con el propósito de difundir *malware*. El correo tiene como asunto: **«comprobante de transferencia bancaria - [id (números aleatorios)]»**. En el cuerpo del mensaje se indica al usuario que se ha producido una transferencia desde su cuenta a favor de la Administración Tributaria con motivo del pago del impuesto sobre la renta de las personas físicas, más conocido como IRPF. Se pide al usuario que descargue el documento de la operación para comprobar si se ha realizado correctamente la misma. Al hacer clic sobre el enlace contenido en el correo, se descarga el archivo comprimido con el nombre **«DEVOLUCION_(números aleatorios)_(caracteres aleatorios).zip»** que contiene el *malware*. Este compromete la seguridad del equipo y facilita al ciberdelincuente el robo de información. No se descarta que existan otras campañas similares que usen el nombre de otras entidades financieras, instituciones o administraciones públicas para conseguir sus fines.
 - Campaña de correos electrónicos que distribuyen *malware* **“Trojan Downloader”**, en los que simulaban proceder del **Ministerio de Trabajo y Economía Social** con la intención de difundir un *malware*.
- El correo, que lleva asociado un archivo adjunto simulando ser un pdf, solicitaba el acceso al ordenador al modificar la configuración de seguridad del equipo infectado.
- Campaña de correos fraudulentos que simulaban ser **del servicio de Correos para hacerse con información bancaria**. En el asunto aparece el mensaje “Su paquete está esperando la entrega”. En este caso informaban de que no se ha podido entregar un paquete y se insta que se reprograme la entrega previo pago a través de un enlace, en el que se cumplimentaban los datos bancarios.
 - Se ha detectado una campaña masiva de envío de correos electrónicos fraudulentos de tipo *phishing* que tratan de suplantar a la plataforma **Ruralvía** de la entidad bancaria Caja Rural.
 - Campaña de correos fraudulentos que **suplantaban a Vodafone** con el fin de **difundir malware**. El correo que suplanta a Vodafone tiene como asunto «Fwd: factura pendiente - Nº (números aleatorios)». En el cuerpo del mensaje se informa al usuario que ha vencido el plazo para pagar la factura en plazo y se le exige que realice el pago antes de la fecha señalada. Además, el correo tiene asociado un archivo adjunto que simula ser una factura que, al pulsar sobre la vista previa, abre el navegador y descarga el archivo comprimido con el nombre **«ARCHIVO_D_(números aleatorios)_(caracteres aleatorios).zip»** que contiene un troyano. Este archivo malicioso compromete la seguridad del equipo, ya que facilita al ciberdelincuente el acceso al mismo al modificar la configuración de seguridad del equipo infectado.
 - Campaña de correos que aparentaban **a la Agencia Estatal de Administración Tributaria (AEAT)**. En la campaña identificada, el correo que se hacían pasar por la AEAT tiene como asunto «Fwd: Servicio Tributaria -(números aleatorios)». En el cuerpo del mensaje se solicita al usuario verificar si el «monto de la factura fiscal es correcto» y se le indica que el plazo de pago ha finalizado. El correo tiene asociado un archivo adjunto que simula ser un fichero pdf que, al pulsar sobre la vista previa, abre el navegador y descarga el archivo comprimido con el nombre **«ARCHIVO_D_(números aleatorios)_(caracteres aleatorios).zip»** que **contiene un troyano**. Este archivo malicioso compromete la seguridad del equipo ya que **facilita al ciberdelincuente el acceso** al mismo al modificar la configuración de seguridad del equipo infectado.

AVISOS EN CIBERSEGURIDAD

FUENTE: INCIBE

El INCIBE recomienda extremar las precauciones. Si se ha realizado el pago debe contactarse con la entidad bancaria en cuestión para informarles de la situación. Se deben recopilar todas las pruebas de las que se disponga (captura de pantalla, e-mail, mensajes, etc) y presentar la denuncia ante las Fuerzas y Cuerpos de Seguridad. Entre las pautas generales destacan:

- No abrir correos de usuarios desconocidos o que no haya solicitado: hay que eliminarlos directamente.
- En caso de que el correo proceda de una entidad bancaria legítima, nunca contendrá enlaces a su página de inicio de sesión o documentos adjuntos.
- No contestar en ningún caso a estos correos.
- Tener precaución al seguir enlaces o descargar ficheros adjuntos en correos electrónicos, SMS, mensajes en WhatsApp o redes sociales, aunque sean de contactos conocidos.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.
- Asegúrate de que las cuentas de usuario de tus empleados utilizan contraseñas robustas y sin permisos de administrador.



LA RED AZUL DE LA POLICÍA ESPAÑOLA EN AMERIPOL

COMISARIO PRINCIPAL, MANUEL YANGUAS MENÉNDEZ

*La Comunidad de Policías de América (AMERIPOL), es un mecanismo de cooperación hemisférico, integrado y coordinado, cuyo propósito es promover y fortalecer la cooperación policial en materia técnico científica, la capacitación, así como dinamizar y hacer más efectivo el intercambio de información con fines de inteligencia. De igual forma, tiene como propósito coordinar y potenciar acciones sostenidas de investigación criminal y asistencia judicial entre los cuerpos de policía y/o instituciones homólogas de América, para que se traduzcan en la consolidación de la doctrina y filosofía policial, así como en la prevención y neutralización del delito. Actualmente está integrado por **33 cuerpos de Policía o Instituciones Homólogas y 26 Organismos Observadores**, los cuales se encuentran distribuidos alrededor de todo el mundo (página oficial de AMERIPOL).*

El pasado día 17 de septiembre, el Jefe de la Unidad Central de Seguridad Privada **D. Manuel Yanguas Menéndez**, mantuvo una reunión virtual con los principales representantes de AMERIPOL con el objetivo general de dar a conocer el **Plan Integral de Colaboración de la Policía Nacional con la seguridad privada, RED AZUL**, así como exponer como se ha llevado a cabo la adaptación de los protocolos de actuación para lograr la cooperación efectiva entre la seguridad privada y la Policía Nacional durante la crisis del COVID-19.

El Jefe de la Unidad Central realizó un breve recorrido histórico por las leyes que se han implementado en España para regular la seguridad privada, y explicó los mecanismos de colaboración concretos, como es el caso de RED AZUL, que busca potenciar la cooperación y coordinación operativa.

Asimismo, hizo alusión a acciones concretas de colaboración como la formación impartida a personal sanitario para prevenir las agresiones que sufren en su labor diaria. A través de **los Interlocutores Policiales Sanitarios de la Policía Nacional**, los profesionales de la salud se forman en técnicas de detección de situaciones violentas y de prevención de las posibles agresiones.

Como próximo objetivo, se está estudiando la creación de una **"RED DE SEGURIDAD PRIVADA"**, liderada por AMERIPOL y la Policía Nacional de España, que aglutinaría a los diferentes cuerpos policiales de América y Europa con competencias en seguridad privada.



EL DETCAMP DETECTIVES 4.0

Entrevista a la UCSP

INSPECTOR JEFE, DAVID BRAVO NÚÑEZ

La plataforma informativa sobre investigación privada, **DETCAMP**, entrevistó al **Inspector Jefe, David Bravo Núñez**, Jefe de la Sección de Operativa Colaboración de la Unidad Central de Seguridad Privada.

La entrevista, dadas las actuales circunstancias sanitarias, se llevó a cabo de forma telemática y como no podía ser de otra manera, giró en torno al mundo de los detectives privados. Se explicó como aunque se hayan reducido el número de las habituales reuniones y contactos personales que se mantenían con los responsables e integrantes de los despachos de detectives privados, el contacto siempre se ha mantenido vía telefónica y una vez terminó el excepcional periodo, de forma progresiva y cumpliendo las normas de prevención y protección sanitaria se ha vuelto a reactivar la actividad.

A lo largo de la misma se abordaron diferentes cuestiones, comenzando con un análisis de la actual situación en que estamos inmersos y cómo nos está poniendo a prueba.

Otro de los aspectos que se abordó en la entrevista fue la entrega de memorias y la reactivación de la actividad inspectora, destacando el hecho de que las inspecciones, en general, están siendo positivas, aprovechando para aclarar ciertas dudas en relación a las mismas.

Una de las preguntas estaba relacionada con datos estadísticos sobre la apertura de despachos, nuevas habilitaciones, etc. por lo que se facilitaron datos comparativos entre el primer semestre de 2020 respecto al mismo periodo de 2019.

La formación que se lleva a cabo en las universidades para obtener la titulación necesaria para habilitarse como detective fue otro de los asuntos que se trataron y se comentaron posibles mejoras en la misma, siempre desde un punto de vista constructivo. A modo de ejemplo, se expuso que debería ahondarse en el conocimiento de la parte administrativa que rige la gestión de los despachos de detectives privados tales como la forma de rellenar el libro correctamente, requisitos de los contratos, etc.

También salió a colación la acción formativa que se llevó a cabo con las principales mutuas y aseguradoras sobre la labor de los detectives, y se preguntó sobre nuevas acciones en ese sentido.

Asimismo se destacó la importancia de utilizar el canal Red Azul como ventana única de comunicación y colaboración de Policía Nacional con el sector de la Seguridad Privada.

El intrusismo, la ciberinvestigación, la renumeración de los despachos de detectives y el futuro reglamento fueron cuestiones que no podían faltar y sobre las que se habló en la entrevista.

Los interesados en ver la entrevista pueden hacerlo a través del siguiente enlace:

<https://youtu.be/vm-eg0x7jiY>



HACKEO DE LLAVES MEDIANTE PATRONES DE SONIDO

FUENTE: NATIONAL UNIVERSITY OF SINGAPORE

La tecnología nos facilita la vida pero también da más herramientas a los delincuentes para cometer actos delictivos.

Actualmente es indispensable que nos protejamos de los hackers y alejarnos de cualquier plataforma online de aspecto sospechoso. Debemos evitar que nuestros datos caigan en manos con siniestras intenciones. Sin embargo, hemos de saber que los temidos ciberataques pueden también tener consecuencias físicas, es decir, hacerse realidad y traspasar la pantalla del ordenador. Se ha descubierto como hackers pueden clonar las llaves de entrada en las casas.

Un trabajo de la National University of Singapore nos explica como funciona el método con las cerraduras de tambor de pines, esto es, aquellas que necesitan la clásica llave de sierra.

Primeramente el atacante llevará a cabo un examen externo para conocer el tipo de cerradura y de llave. Después deberá grabar el sonido de la llave al entrar en la cerradura.

La llave, al ser introducida en la cerradura por el dueño del inmueble, va empujando los resortes de la cerradura a diferentes alturas, para que los mismos queden alineados y el tambor gire y se abra la misma. Es precisamente el ruido que hace la llave al introducirse en la cerradura e ir empujando los resortes, en lo que se basa el “hackeo” de la llave.

Así, con una simple grabación de ese sonido, los delincuentes pueden establecer su patrón. Cuando una víctima inserta la llave en la cerradura, emite un sonido que es capturado por el sistema de grabación de audio del delincuente.

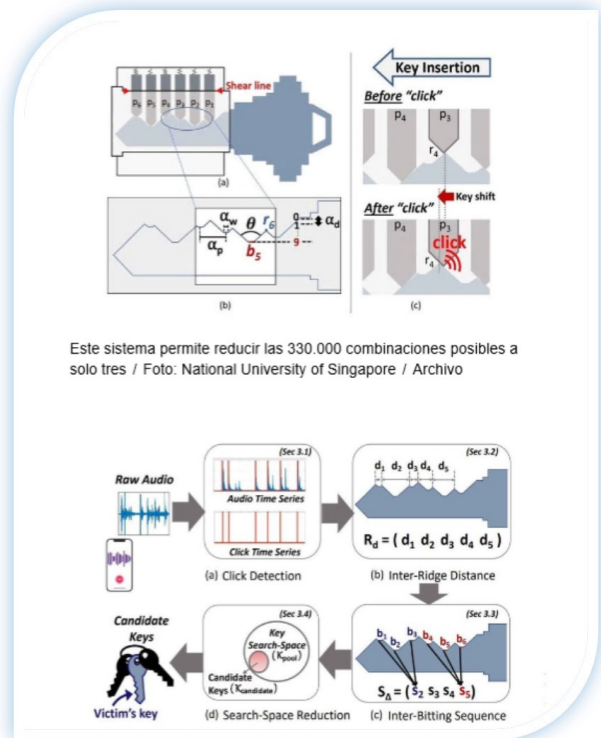
Según estudios realizados, este sistema es capaz de reducir el número de llaves candidatas de 330.000 a tan sólo tres. Seguidamente, el atacante imprimirá el diseño de los modelos obtenidos y probará hasta dar con el que le funciona.

Los sonidos captados por el “hacker”, es decir, los que se producen al meter la llave en la cerradura, son de baja frecuencia, por lo que deben utilizar una aplicación que a la vez que capture los sonidos, elimine el ruido de ambiente.

El talón de Aquiles de este método es que se requiere que la llave se introduzca en la cerradura a una velocidad constante, para después, utilizando ingeniería inversa al sonido, se puedan reproducir los patrones y confeccionar la llave. Esta debilidad del método es lo que se tiene que aprovechar para evitar que nos dupliquen la llave. Por ello se recomienda introducir la llave con diferentes movimientos y nunca de forma uniforme, a la vez que se pue-

de “contaminar” el sonido ambiente con algún ruido que podamos hacer, con la música de nuestro móvil, o simplemente silbando una canción.

Para más información, seguir el siguiente enlace: https://youtu.be/bxyAa_txM34



DRONES: ENTREVISTA AL GRUPO PERSEO

Policía del Aire

La Unidad Central de Seguridad Privada mantuvo una reunión con el **Inspector José Luis Boto**, responsable del Grupo Perseo de la Policía Nacional, dedicado a la detección y neutralización de RPA's (drones) que realicen vuelos no autorizados.

¿Dónde está enmarcado el Grupo Perseo y cuáles son sus misiones?

El Grupo Perseo está dentro del Área de Telecomunicación de la Unidad de Informática y Comunicaciones de la Policía Nacional.

Además de las tareas propias que venimos realizando de forma habitual, en estos últimos años se nos ha asignado la misión de detectar, localizar y neutralizar, en su caso, drones que violen el espacio aéreo mediante vuelos no autorizados. Es por ello que en la celebración de eventos deportivos de especial relevancia u otros acontecimientos que congreguen a una gran cantidad de personas, tenemos la misión de mantener la seguridad del espacio aéreo en lo que a vuelo de drones se refiere.

¿Está prohibido utilizar drones?

Aunque no sea el objetivo de esta entrevista, tengo que hacer referencia a la normativa reguladora, concretamente el *Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto*, que determina que dichas aeronaves no pueden poner en riesgo ni la seguridad aérea, ni la de las personas y objetos que estén debajo de la nave pilotada por control remoto. Y en relación al uso recreativo de los drones establece que:

- No pueden volar sobre aglomeraciones de edificios, en ciudades, pueblos y lugares habitados o de reuniones al aire libre excepto cuando se trate de drones hasta 250 gramos con una altura de vuelo hasta 20 metros.
- No pueden volar a una distancia mínima de 8 km respecto al punto de referencia de cualquier aeropuerto o aeródromo.
- No pueden volar en los espacios aéreos controlados, prohibidos o restringidos.

Por otro lado, quiero puntualizar algo que la mayor parte de los vecinos de Madrid desconoce: **En Madrid está prohibido volar drones.**

En caso de ser necesario realizar vuelos con drones en la capital, la Agencia Estatal de Seguridad Aérea (AESA), puede conceder un permiso para llevar a cabo esos vuelos, pero, sólo en determinadas zonas y siempre y cuando se esté en posesión de la titulación correspondiente. Luego existen otras zonas en las que está completamente prohibido y AESA no concede permisos

para utilizarlos en las mismas, como es el caso del Palacio Real y sus inmediaciones o la zona de La Moncloa.

¿Cómo de peligroso puede llegar a ser un dron?

Podemos pensar que el tamaño de un dron comparado con un avión es insignificante, y que por ello es inofensivo para la aeronave, lo cual es completamente erróneo.

No hace demasiado tiempo se dio el caso de un avión que una vez había despegado, le reventó una rueda y parte del material de la misma, entró en el motor, viéndose el comandante del avión obligado a volver a aterrizar.

Podría suceder lo mismo con un dron, el cual podría entrar en el motor o golpear contra uno de sus cristales, pudiendo causar daños importantes al mismo. Un dron puede hacer mucho daño a una aeronave y causarle averías importantes.

Debemos pensar, que **los drones no son un juguete.**



Explicanos el sistema de detección de drones que hay desplegado en Madrid.

Madrid es la primera ciudad de Europa en la que se ha implantado un sistema de detección de drones, denominado CAELUS. El sistema está gestionado a través de la Secretaría de Estado de Seguridad y permite detectar el dron desde el momento mismo en que el piloto pone en marcha el dispositivo aéreo. Por la ciudad se han establecido de forma estratégica diferentes antenas receptoras, estando una de ellas ubicada en las instalaciones del CIMACC 091. Las antenas detectan la presencia del dron, obteniendo información del dispositivo aéreo, así como ubicación de la controladora y del piloto. Todo ello en tiempo real. La precisión en la ubicación es máxima, pudiendo decirse que apenas existe error en la misma.

DRONES: ENTREVISTA AL GRUPO PERSEO

Policía del Aire

¿Son los drones un instrumento útil?

Sin lugar a dudas. Lo más importante es quien los maneja y con que finalidad.

La Policía Nacional dispone de drones, los cuales son de máxima utilidad para seguimientos, visualización de lugares de difícil acceso en los registros, obtención de imágenes de zonas donde otros sistemas no son capaces de llegar, búsqueda de personas, en la lucha contra el narcotráfico, seguridad en eventos, etc.



El Servicio de Medios Aéreos de la Policía Nacional es el competente de todo lo relacionado con drones, desde la formación y titulación correspondiente, al manejo de los mismos. Como ya he dicho, un dron no es un juguete, y su manejo requiere conocimientos, pericia y precaución. Una hélice de un dron puede causar daños graves en las manos de una persona inexperta o sin las competencias correspondientes.

¿Y que infracciones puede cometer alguien que levante un RPA sin los permisos y autorizaciones requeridas?

Pues son infracciones que pueden afectar a tres planos normativos distintos.

Primeramente, y como hemos dicho, se ve afectada la seguridad aérea, por lo que se infringe la normativa reguladora de la misma. Después, se ve afectada la seguridad ciudadana en general. Y finalmente, el hecho que estos dispositivos aéreos disponga de cámaras de captura de imágenes y video, hace que sean susceptibles de ser utilizados para cometer delitos contra la intimidad, ya que permiten obtener fotos y videos de lugares donde las personas desarrollan su vida íntima, lo cual sólo su grabación ya podría ser motivo de reproche penal, y más cuando a esas grabaciones se les da difusión a través de redes so-

ciales, o de medios de comunicación, lo que podría dar lugar al delito de descubrimiento y revelación de secretos.

De especial relevancia es la aplicación de la **Ley 21/2003, de seguridad aérea**, que en su régimen sancionador dispone la imposición de multas, que en el caso de las graves y muy graves, pueden llegar a 90.000 y 225.000 euros respectivamente; y en el caso de que el piloto del RPA sea un profesional en posesión de las titulaciones correspondientes, las anteriores cuantías se incrementan hasta los 250.000 y los 450.000 euros.

Por otro lado, y como he explicado, los RPA'S son unos instrumentos muy versátiles, y se ha descubierto como los delincuentes pueden utilizarlos para tratar de introducir objetos en cárceles u otros lugares donde no es fácil acceder, para depositar teléfonos móviles, drogas, explosivos o algún otro tipo de material prohibido.

¿Estamos preparados para la lucha contra el uso ilegal de drones?

Trabajamos para que así sea. Estamos tratando de potenciar al máximo la formación y actualización de los policías que nos dedicamos específicamente a ello. No obstante, y es una percepción personal, la Policía Nacional está a la cabeza de Europa en cuanto a conocimientos y procedimientos de la lucha contra el uso ilícito de drones.



La Unidad Central de Seguridad Privada, como Autoridad Nacional de Control, ha recibido y sigue recibiendo consultas en relación a las instalaciones de sistemas de circuito cerrado de televisión en comunidades de propietarios, su mantenimiento y su visionado por personal distinto del personal de seguridad. Es por ello, por lo que se estima oportuno hacer un recorrido por lo que estipula la normativa de seguridad privada al respecto, así como recordar el pronunciamiento que hizo la Unidad Central en relación con ese asunto y que se plasmó en el informe 2018_004, de carácter informativo, orientativo y nunca vinculante.

La primera parada en el recorrido normativo debemos hacerla en el **artículo 5 “Actividades de seguridad privada”, de la Ley 5/2014, de 4 de abril, de Seguridad Privada (LSP)**. Dicho artículo determina que “La vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos” es una actividad de seguridad privada y los servicios sobre esa actividad únicamente pueden prestarlos empresas de seguridad privada, sin perjuicio de las competencias de las Fuerzas y Cuerpos de Seguridad.

Asimismo, el **artículo 42 “Servicios de videovigilancia”** de la LSP explica que dichos servicios consisten en ejercer la vigilancia a través de sistemas cámaras o videocámaras y que, cuando la finalidad de estos servicios sea la prevención de infracciones o evitación de daños o impedir accesos no autorizados, serán prestados por vigilantes de seguridad o, en su caso, por guardas rurales.

Por otro lado no se considera videovigilancia si el objeto principal es la comprobación de estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje, por lo que estas funciones podrán realizarse por personal distinto al de seguridad privada.

Por otro lado, el **Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada**, define en su **artículo 39** los centros de control como aquellos lugares donde se centralizan los sistemas de seguridad y vigilancia de un edificio o establecimiento, debiendo estar controlados por personal de seguridad privada.

En base a lo expuesto, el lugar donde se ubiquen los monitores tendrá la consideración de centro de control cuando el servicio prestado sea de vigilancia y protección de bienes y personas en general, y en este caso, la instalación y mantenimiento de los sistemas de videovigilancia siempre deberá realizarse por empresas de seguridad autorizadas para estas actividades. Es decir, que la consideración de centro de control, viene determinada no por el hecho de instalar un sistema de CCTV, sino por el

visionado en tiempo real de las imágenes generadas por esas cámaras y siempre que éstas tengan esa finalidad preventiva o de vigilancia para tratar de dar respuesta a la comisión de hechos presuntamente delictivos.



Es por ello que, el visionado, en tiempo real, de las imágenes obtenidas por los sistemas de CCTV instalados en una comunidad de vecinos, **cuando éstas tengan como finalidad la vigilancia y prevención de posibles hechos delictivos**, solo podrá hacerse por vigilantes de seguridad o bien transmitir las imágenes a una empresa autorizada para la actividad de centralización de alarmas.

Los auxiliares de control, conserjes, porteros o similares de una comunidad de propietarios podrían visionar los monitores de un sistema de circuito cerrado de televisión **cuando la finalidad de estos servicios sea distinta** a la prevención de infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados.

El tratamiento de las imágenes originadas por dichos sistemas y almacenados en dispositivos grabadores, estarán sometidos a la regulación específica de la protección de datos de carácter personal.

SERVICIO DE VERIFICACIÓN PERSONAL DE ALARMAS

INSPECTOR JEFE , FRANCISCO JOSÉ ALONSO TEJEDA

Introducción

Con el objetivo de desarrollar la colaboración entre la Seguridad Pública y la Seguridad Privada, desde la Unidad Central de Seguridad Privada se ha estimado relevante que, mediante las posibilidades que permite el Boletín "R@S", canalizar una serie de publicaciones, en las que exponiendo, de una forma breve y sencilla, se pueda visibilizar y clarificar las condiciones, requisitos y otras circunstancias, que la normativa establece sobre cómo deben desarrollarse determinados servicios de seguridad privada, y consecuentemente con ello, se facilite el correcto funcionamiento de los diferentes tipos de servicios. En este sentido, se ha considerado adecuado iniciar esta actividad de colaboración exponiendo las características y otras consideraciones sobre los servicios de verificación personal de alarmas y respuesta a las mismas, comúnmente conocidos como servicios de acuda.

De igual forma, es de significar que, el presente artículo tiene un carácter meramente informativo y orientativo, sin que quepa atribuir al mismo otros efectos o aplicaciones distintos del mero cumplimiento del deber de servicio a los ciudadanos.

Consideraciones

1. Actividad

El servicio denominado "respuesta ante alarmas", se encuentra dentro de la actividad descrita en el artículo 5.1.g) de la Ley 5/2014, de Seguridad Privada (en adelante LSP), que consiste en *"La explotación de centrales para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma, así como la monitorización de cualesquiera señales de dispositivos auxiliares para la seguridad de personas, de bienes muebles o inmuebles o de cumplimiento de medidas impuestas, y la comunicación a las Fuerzas y Cuerpos de Seguridad competentes en estos casos"*.

Si bien, esta es una actividad reservada, en aplicación de lo dispuesto en el propio artículo 5 de la LSP en su apartado 2, para ser desarrollada por empresas de seguridad, es también esta Ley, la que permite que las entidades públicas o privadas puedan constituir, previa autorización del Ministerio del Interior o del órgano autonómico competente, centrales receptoras de alarmas de uso propio para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma que reciban de los sistemas de seguridad instalados en bienes inmuebles o muebles de su titularidad.

2. Servicios

La actividad de explotación de centrales receptoras de alarmas, posibilita el desarrollo de los siguientes servicios:

1. **De gestión de alarmas**, que consistirá en la recepción, verificación no personal y, en su caso, transmisión de las señales de alarma relativas a la seguridad y a la protección de personas y bienes, a las Fuerzas y Cuerpos de Seguridad competentes. Este servicio será prestado por operadores de seguridad, pudiendo ser, asimismo realizado por vigilantes de seguridad.
2. **De respuesta ante alarmas**, que solo pueden ser prestados por vigilantes de seguridad o guardas rurales, y que a su vez se compone de los siguientes servicios de seguridad:
 - a. El depósito y custodia de las llaves de los inmuebles u objetos donde estén instalados los sistemas de seguridad conectados a la central de alarmas y, en su caso, su traslado hasta el lugar del que procediere la señal de alarma verificada o bien la apertura a distancia controlada desde la central de alarmas.
 - b. El desplazamiento de los vigilantes de seguridad o guardas rurales a fin de proceder a la verificación personal de la alarma. Permitiendo dos modalidades:
 - Verificación mediante la inspección exterior del inmueble o local protegido, que puede ser realizada por al menos un vigilante de seguridad o, en su caso, guarda rural.
 - Verificación interior del local o instalación protegida, en cuyo caso deberá ser realizada, como mínimo, por dos vigilantes de seguridad o, en su caso, guardas rurales.
 - c. Facilitar el acceso a los servicios policiales o de emergencia cuando las circunstancias lo requieran, bien mediante aperturas remotas controladas desde la central de alarmas o con los medios y dispositivos de acceso de que se disponga.



SERVICIO DE VERIFICACIÓN PERSONAL DE ALARMAS

3. Custodia de las llaves

La custodia de las llaves de acceso a las instalaciones objeto de protección, de este tipo de servicio, admite las siguientes modalidades de “resguardo o custodia”, debiendo:

- **En el interior centro de control** de la empresa de central receptora de alarmas o, en su caso, de la entidad con central de alarmas de uso propio.
- **En caja fuerte**, dentro de la sede o delegación de empresa de seguridad, tanto si se trata de la central receptora de alarmas o de la empresa subcontratada de vigilancia y protección, o en las instalaciones donde se ubique la entidad con central de alarma de uso propio (para aquellos casos en los que la custodia se lleve a cabo fuera del centro de control).
- **En vehículo**, previamente autorizado por el servicio policial, en este caso las llaves deben estar obligatoriamente codificadas, y deben ser custodiadas por vigilantes de seguridad.

4. Vigilantes de seguridad

Los vigilantes de seguridad que desarrollan estos servicios de verificación y respuesta, si bien pueden pertenecer a la plantilla de la empresa de seguridad con la actividad de explotación de central receptora de alarmas, la normativa permite la subcontratación con una empresa de seguridad autorizada para desarrollar la actividad de vigilancia y protección, aun no existiendo la identidad de dedicación de las empresas para subcontratar, como exige el artículo 14 del Reglamento de Seguridad Privada.

En el caso de tratarse de entidades con central de alarmas de uso propio, al no tener la consideración de empresa de seguridad, no pueden contratar directamente vigilantes de seguridad para el desarrollo de este servicio, por lo que deberán, en su caso, contratar la prestación del servicio con una empresa de seguridad autorizada para la actividad de vigilancia y protección.

Como norma, los vigilantes de seguridad habrán de prestar este tipo de servicio sin arma, si bien, está previsto la posibilidad que los cuerpos policiales competentes, o las autoridades previstas en el artículo 81 del Reglamento de Seguridad Privada, autoricen el uso de sistemas y medios de protección y defensa distintos a los habituales, incluida el arma de fuego reglamentaria.

Deben desarrollar este servicio ostentando el distintivo del cargo, vistiendo la uniformidad autorizada y portando los medios de defensa reglamentarios o en su caso, autorizados.

5. Caja fuerte

La caja fuerte utilizada para la custodia de las llaves, ubicada en la sede o delegación de la empresa de seguridad (central receptora de alarmas o la subcontratada de vigilancia y protección) o en las instalaciones donde radique la central de alarmas de uso propio, debe disponer de las siguientes características de seguridad:

- Grado de seguridad 3, según la Norma UNE-EN 1143-1.
- Cuando la caja fuerte pese menos de 2.000 kilogramos, deberá estar anclada de manera fija al suelo o pared, conforme a lo establecido en las disposiciones adicionales segundas de la Orden INT/314/2011 sobre empresas de seguridad y de la Orden INT/317/2011, sobre medidas de seguridad privada.

6. Vehículos utilizados para llevar a cabo el traslado o



custodia de llaves

De forma general deben cumplir con los siguientes requisitos:

- No podrán utilizarse vehículos que no sean de la empresa de seguridad, debiendo estar rotulado con anagrama de la empresa de seguridad.
- Deberán llevar un sistema (vía radio-teléfono) que permita la comunicación con la central receptora de alarmas, con el objeto de informar de las incidencias o situación observada.
- Sus características, no permitirán confundirse con los de las Fuerzas Armadas ni con los de las Fuerzas y Cuerpos de Seguridad.
- Tampoco pudiendo disponer de lanza-destellos o sistemas acústicos destinados a obtener preferencia de paso a efectos de circulación vial.

De forma específica, para cada uno de los casos expuestos:

- **Servicio de traslado de llaves** desde la sede/delegación de la empresa de seguridad o local de la central de alarmas de uso propio al bien protegido:

- No requieren autorización previa del vehículo utilizado.

- **Servicio de la custodia de llaves en el propio vehículo:**

- Requiere autorización previa del vehículo por los servicios policiales donde se vaya a llevar a cabo el servicio.
- Obligación de codificación de las llaves y modificación periódica una vez al semestre o cada vez que sean utilizadas.
- Llaves protegidas por el/los vigilantes de seguridad.

7. Formación

El personal de seguridad privada que preste este tipo de servicio, deberá recibir la formación específica, como señala el Anexo IV de la Orden INT/318/2011, sobre personal de seguridad privada, salvo que hubiese encontrado desempeñando este tipo de servicio dos años antes de la entrada en vigor de la citada Orden.

Normativa aplicable:

Ley 5/2014, de Seguridad Privada: artículos 5.1.g), 5.3, 9, 32.1.f), 34, 40.2, 47.2.

R. D. 2364/1994, por el que se aprueba el Reglamento de Seguridad Privada: artículos 14, apartados 3 y 4, 18, 24.c), 47, 48.2, 49.

Orden INT/314/2011, sobre empresas de seguridad privada: artículos 12.3, 25, Disposición adicional segunda que establece el anclaje de las unidades de almacenamiento.

Orden INT/316/2011, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada: artículos 12, 17, 18.

Orden INT/318/2011, sobre personal de seguridad Privada: artículo 8, relativo a la formación específica del personal de seguridad privada.

Resolución de 12 de noviembre de 2012, de la Secretaría de Estado de Seguridad, por la que se determinan los programas de formación del personal de seguridad privada:

- Parte dispositiva, donde se amplía los servicios que requieren de una formación específica, como es el relativo al de verificación personal de las alarmas.
- Primero. Apartado que establece los contenidos mínimos de los programas de formación específica.
- Anexo II, Apéndice 2, que establece la formación específica para Vigilantes de Seguridad que presten servicio de respuesta ante alarmas.



ENTREGA DE MENCIONES HONORÍFICAS A DOS VIGILANTES DE SEGURIDAD

La Policía Nacional entregó dos menciones honoríficas a dos profesionales de la seguridad privada por la detención de un individuo armado.

Ángel y Roberto son dos vigilantes de seguridad que desarrollan su servicio en la red de trenes de cercanías de Madrid y que consiguieron resolver de forma brillante una peligrosa intervención.



Cuando se encontraban prestando servicio, fueron requeridos por los viajeros de un vagón que les informaron de la presencia de un individuo que, armado con un cuchillo, amenazaba a los ocupantes del tren.

Ambos, teniendo siempre presente la alta ocupación del medio de transporte, consiguieron reducir al individuo sin que nadie sufriera ningún daño.

Dos vigilantes de seguridad que, exponiendo su propia integridad, han sido reconocidos por haber sobresalido en el cumplimiento de sus obligaciones.



LA POLICÍA DEL AIRE EVALÚA LOS SISTEMAS ANTIDRÓN EN EL AEROPUERTO DE ASTURIAS

Entre el 14 y 18 de septiembre, se llevaron a cabo en el aeropuerto de Asturias unas pruebas, organizadas por la Secretaría de Estado de Seguridad del Ministerio del Interior, en las que se evaluaron diversos sistemas antidrón, con el fin de conocer las diferentes opciones tecnológicas existentes en el mercado y comprobar si haciendo frente

a la amenaza de los drones, no interferían en operatividad de la navegación aérea.

En su organización participaron representantes de los ministerios de Defensa y Transportes, Movilidad y Agenda Urbana, así como especialistas de Policía Nacional, de Guardia Civil, Mossos d'Esquadra y Ertzaintza y técnicos de la Agencia Estatal de Seguridad Aérea (AESA) y las empresas públicas del sector aeroportuario, AENA y ENAIRE.

Para hacer frente al riesgo que supone el uso de los drones para actividades ilegales, y siguiendo la Estrategia de Seguridad Nacional, la Secretaría de Estado de Seguridad puso en marcha en julio de 2019 la creación de una red de sistemas de detección y, en su caso, de neutralización de drones llamado Sistema Global Contra Drones (SIGLO-CD), que detecta, identifica y monitoriza las aeronaves de este tipo más comunes del mercado. El despliegue del sistema ha permitido detectar y neutralizar más de 9000 vuelos de drones.

Visualizar el video que se adjunta con el presente boletín.



LA POLICÍA NACIONAL EN LA JORNADA "CONSECUENCIAS JURÍDICO SANITARIAS DE LA CRISIS DEL COVID-19"

El día 1 de octubre, se celebró en el Paraninfo de la Universidad CEU Cardenal Herrera de Afara del Patriarca (Valencia) la jornada "Consecuencias Jurídico Sanitarias de la Crisis del Covid 19", organizada por la Asociación de Derecho Sanitario de la Comunidad Valenciana.

En la misma intervino el Interlocutor Policial Nacional Sanitario de la Policía Nacional, Comisario Javier Galván Ruiz.

Durante la conferencia expuso como la Policía Nacional llevó a cabo la implantación de la figura del Interlocutor Policial con el sector sanitario y, seguidamente, presentó el trabajo realizado por los Interlocutores Sanitarios de la Policía Nacional durante el estado de alarma.

La realización de 8.000 contactos con los principales actores del sector sanitario, la gestión de los dispositivos de protección de transporte de material sanitario y el asesoramiento sobre el **botón SOS de la aplicación Alert-cops**, fueron, entre otras, las acciones llevadas a cabo por los Interlocutores Policiales Sanitarios de la Policía Nacional durante los casi tres meses de confinamiento.



OPERACIÓN POLICIAL CONTRA EL INTRUSISMO EN EL SECTOR DE LA SEGURIDAD PRIVADA EN LA PROVINCIA DE CÁDIZ

La Policía Nacional ha detenido a una persona como presunta autora de un delito contra la Administración Pública y tenencia ilícita de armas, que prestaba servicio de manera ilegal en una empresa de seguridad y se ha propuesto para sanción a unos falsos vigilantes por infracción de la Ley de Seguridad Privada.

La empresa de seguridad, autorizada por el Ministerio del Interior, estaba contratada para un servicio de vigilancia y protección con armas en una explotación agrícola, en la que de manera paralela, el propietario había establecido un servicio de seguridad ilegal desempeñado por dos personas sin habilitación profesional de vigilantes y que además carecían de contrato de trabajo.

A los falsos vigilantes les han sido intervenidos, entre otros efectos, una pistola con tres cargadores y 82 cartuchos de 9mm, así como una pistola de simulada, una defensa eléctrica, equipos de comunicaciones portátiles, dos navajas militares de grandes dimensiones y unos grilletes.



ENTREGA DE MENCIÓN HONORÍFICA A UN VIGILANTE DE SEGURIDAD QUE SALVÓ LA VIDA DE UN CIUDADANO

El pasado 1 de octubre, la **Policía Nacional** entregó una **mención honorífica a Fermín, vigilante de seguridad** con larga experiencia profesional que desarrolla su labor en un centro de acogida. Durante uno de sus servicios, un usuario del centro entró en parada cardiorrespiratoria.

Gracias a su rápida reacción, llevando a cabo técnicas de RCP (reanimación cardiopulmonar) y utilizando un desfibrilador, mantuvo con vida al ciudadano hasta la llegada de los servicios sanitarios, que consiguieron su recuperación.



FORMACIÓN A PERSONAL DE SEGURIDAD PRIVADA

La Unidad Central de Seguridad Privada, adaptándose a los condicionantes de la actual situación sanitaria, ha iniciado una **actividad formativa on-line** en el marco de la formación especial, impartiendo unas jornadas de formación en **materia de prevención antiterrorista y la colaboración entre la seguridad pública y privada dirigida a vigilantes de seguridad**.

Dichas jornadas se celebrarán durante los meses de octubre, noviembre y diciembre invitando a todos los vigilantes interesados a participar en ellas.

Actualmente se siguen impartiendo, a petición de los diferentes actores del sector de la seguridad privada, conferencias presenciales en grupos reducidos, manteniendo en todo momento las medidas de seguridad sanitaria.



DESARTICULADA UNA ORGANIZACIÓN TRANSNACIONAL DEDICADA AL BLANQUEO DE BENEFICIOS PROCEDENTES DE CIBERATAQUES Y ESTAFAS INFORMÁTICAS

La Policía Nacional, Mossos d'Esquadra y FBI, en una operación coordinada por EUROPOL, han desarticulado **una organización transnacional** dedicada al blanqueo de beneficios procedentes de **ciberataques y estafas informáticas que operaban a nivel mundial**.

Esta operación policial internacional ha supuesto la práctica de cuarenta registros domiciliarios y la **detención de 19 personas**. El entramado en nuestro país se había servido de 106 cuentas bancarias, abiertas con pasaportes falsificados, que recibían grandes cantidades de dinero asociadas a actividades de ciberdelitos desde países como Alemania, Italia o Estados Unidos, y con los que pretendían blanquear más de 825.000 euros.

Este entramado criminal ofrecía un servicio consistente en aportar una serie de cuentas bancarias controladas por mulas, previamente reclutadas en varios países por miembros de la organización. La primera finalidad era la de recibir transferencias de dinero procedente de estafas informáticas, así como la de garantizar a los ciberdelinquentes la aplicación de métodos para enmascarar el origen ilícito del dinero y avalar la integración de los beneficios del delito en los circuitos financieros legales.

Gracias a las gestiones de investigación, se pudo identificar un total de 27 personas, que actuaban como mulas bancarias, abriendo cuentas en sucursales bancarias de Barcelona con documentación obtenida fraudulentamente en connivencia con una gestoría establecida cerca de dicha ciudad. Desde esta localidad se realizaban transferencias a cuentas de otros países para enmascarar el origen ilícito y dificultar su rastreo.

Con todas las pruebas recabadas se estima que la actividad de blanqueo llevada a cabo en España superaría los 800.000 euros en un solo año.

