BOLETÍN R@S

NÚMERO 28 MAYO 2023

UNIDAD CENTRAL DE SEGURIDAD PRIVADA

21 DE MAYO, DÍA DE LA SEGURIDAD PRIVADA

365 DÍAS DE VOCACIÓN HACIA LOS DEMÁS

DÍA DE LA SEGURIDAD PRIVADA

Desde la Policía Nacional queremos felicitar en este día especial a todas las personas que forman parte de la familia de la seguridad y la investigación privada de la que también nos sentimos integrantes, siendo nuestro principal lazo de unión y seña de identidad la protección de las personas y bienes de nuestro país.

En este día, 21 de mayo, queremos disfrutar con vosotros de la satisfacción de viajar juntos y pertenecer a un gran colectivo y, con estas palabras, rendir un homenaje a nuestros compañeras y compañeros por su entrega, dedicación y sacrificio.

La Policía Nacional quiere transmitiros **ánimo para que sigáis trabajando como lo habéis hecho hasta ahora, para que las adversidades no dinamiten ni vuestra vocación, ni vuestro empeño** por hacer las cosas de la manera correcta y, juntos, dar respuesta a las necesidades, tanto de investigación como de seguridad privada, que la ciudadanía os demanda, innovando y aportando soluciones a obstáculos que parecen insalvables, consiguiendo con ello que crezca el respeto y la admiración que sienten por aquellos que hacemos que el mundo sea más seguro.

Os estamos agradecidos y os pedimos que sigáis estando ahí, pero que hoy disfrutéis de manera especial de vuestro día en compañía de vuestros seres queridos. La Policía Nacional necesita vuestro apoyo.

FELIZ DÍA DE LA SEGURIDAD PRIVADA

Día de la Seguridad Privada en Cantabria (mayo 2023)

Día de la Seguridad Privada en Murcia (mayo 2023)

AUTOR: José Ignacio Olmos Casado. RENFE

En la actualidad la organización y tendencia, tanto en el día a día como en el cumplimiento de sus objetivos futuros, de los departamentos de seguridad corporativos, se articula en base a las siguientes características:

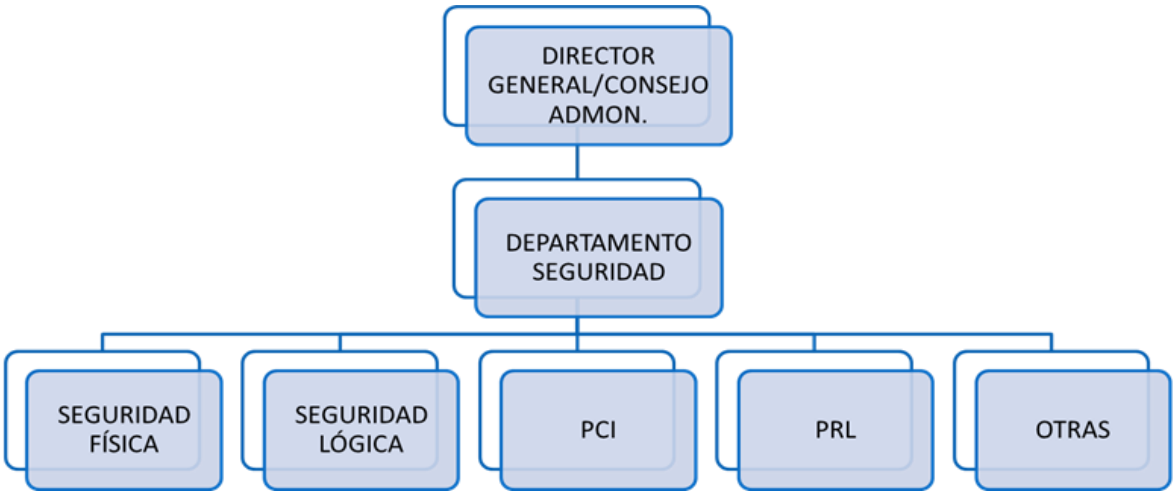
- **El director de seguridad como gestor de riesgos**: más allá de lo que la normativa nacional de seguridad privada establece entre sus funciones el director de seguridad se ha convertido, siguiendo el modelo anglosajón, en un gestor de los diferentes riesgos que pueden afectar a su corporación, aglutinando las diversas ramas de la seguridad integral. En ese modelo ideal de organización, que aún no es predominante entre las compañías, Seguridad depende de la Alta Dirección y todas las materias de seguridad dependen de ella.

- **La seguridad como proceso científico**: la seguridad no es un proceso aleatorio, ni una moda como parece darse con frecuencia hoy día en la instalación de sistemas, sino que es un proceso científico basado en la lógica; por eso es necesario un estudio detallado y un análisis de riesgos adecuado antes de implantar cualquier tipo de medidas; es por eso que la construcción del modelo debe girar en torno al director de seguridad como profesional reputado y de una alta cualificación, que debe ejercer un rol absolutamente basado en el liderazgo respecto de su equipo y del departamento que dirige, asumiendo responsabilidades y ejecutando la toma de decisiones.

- **Dependencia de la Alta Dirección**: el director del departamento de seguridad debe tener dependencia directa del más alto estamento ejecutivo de la compañía, debido a la criticidad para la empresa de las materias que son competencia de su departamento. El director de seguridad debe ser un elemento recurrente en las acciones de importancia de la compañía, adoptando una posición estratégica dentro de la misma.

- **Objetivos del departamento de seguridad en sintonía con los objetivos de la compañía:** el departamento de seguridad no debe ser una isla dentro de la organización, no puede hacer la guerra por su cuenta ni tener unos objetivos propios diferentes de los de la compañía. Los objetivos del departamento tienen que estar alineados con los de la corporación, ya que, como cualquier departamento de la compañía, sirve a los intereses de esta. Eso pasa por la necesidad imperiosa de conocer el negocio, tanto a nivel de sector como de funcionamiento interno de la propia empresa donde está encuadrado.

- **El Departamento de Seguridad como parte de la empresa**: seguridad es un Departamento más de la empresa y puede aportar valor diferencial a la organización (Modelo ESRM-Enterprise Security Risk management).



AUTOR: José Ignacio Olmos Casado. RENFE

Los directores de seguridad deben hablar el mismo lenguaje que el resto de los directivos para tener peso en el Comité de Dirección.

- **Evolución hacia un sistema de gestión**: paso de un modelo mecanicista, que considera a la seguridad como un servicio, producto o persona, hacia un **modelo de gestión** que considera **la seguridad como un proceso estratégico**, utilizando una **metodología** basada en la gestión de la calidad.

Modelo "A"
(management)

- Considerando la seguridad como un objetivo estratégico.
- Utilizando una metodología de gestión adecuada, basada en la gestión de la calidad.
- Gestionando la seguridad como un proceso.

Fuente: José Manuel García Diego

Modelo "B"
(mecanicista)

- Considerando a la seguridad como un servicio (general, complementario)
- Como un producto (cerradura, barrote, CCTV) ó
- Como una persona (VS o DS)

- **Aprovechamiento de la tecnología**: el avance que supone la tecnología permite llegar más lejos y optimizar los recursos, reduciendo presupuestos.

- **Big data**: Tratamiento del dato como elemento esencial para conocer qué está pasando en tiempo real, y que apoya en la toma de decisiones y ayuda a justificarlas.

En la actualidad, respecto a los servicios de seguridad y lo que apuntábamos anteriormente, se dan las siguientes características:

- Tendencia generalizada a la **disminución de servicios armados**, excepto donde existe obligación legal y en las infraestructuras críticas.

- Importante **disminución de los servicios de vigilancia puros** tal y como venían concibiéndose tradicionalmente. Los avances tecnológicos permiten disminuir el elemento humano y, además, financieramente los medios técnicos pueden amortizarse; por tanto, nos encaminamos a un escenario en que se realiza una combinación de la tecnología con el recurso humano.

- En consonancia con lo anterior se está produciendo una **transformación de la vigilancia en supervisión**, realizando servicios en remoto y por otro lado dando servicio de respuesta concretas ante incidentes; como vemos hay disminución de los elementos humanos por un lado y una transformación de estos por otro, acompañados del respaldo técnico y de las posibilidades que permite la tecnología.

- Importancia de la **especialización del director de seguridad** como profesional cualificado y de su liderazgo en la gestión de los especialistas de su equipo como recurso.

- Conforme a las dos premisas anteriores, es imprescindible la **adecuada formación en todos los niveles** y particularmente en el ámbito tecnológico dentro de la vigilancia y en el ámbito del liderazgo en los directivos de seguridad.

LA VENTANA DEL R@S: TENDENCIAS DE GESTIÓN DE LA SEGURIDAD EN GRANDES CORPORACIONES

AUTOR: José Ignacio Olmos Casado. RENFE

Bajo mi punto de vista, en ese entorno cambiante se dan nuevas amenazas que nos obligan a buscar nuevas soluciones en materia de seguridad y de su gestión.

Entre las nuevas amenazas podemos señalar:

- **Entorno VUCA:** hace referencia a los términos en inglés: Volatility, Uncertainty, Complexity and Ambiguity. Volatilidad (volatility). En la realidad actual, sobre todo aplicado al entorno empresarial, es la velocidad a la que se puede producir una gran cantidad de cambio.

- **Crisis:** en la actualidad y tras la pandemia del Covid se está dando no sólo en el ámbito económico, sino también hay una crisis de valores, un choque cultural importante fruto de la globalización, y una crisis existencial en lo personal que está repercutiendo en el mercado laboral.

- **Globalización:** como señalábamos, para lo bueno y lo malo la globalización afecta y se globalizan también las amenazas (movimientos migratorios, delincuencia organizada internacional, ciberdelincuencia…).

- **Aumento de la delincuencia,** como consecuencia de algunos de los factores señalados antes, que provocan y van a seguir provocando cada vez mayores disturbios sociales.

- **Terrorismo Internacional,** sigue estando presente, en particular el de etiología yihadista, con algunos pequeños repuntes locales.

- **El ciberespacio** como nuevo campo de juego para los delincuentes.

Estas nuevas amenazas nos obligan a nuevas soluciones, tecnológicas, digitalización, normalización...

Estas nuevas amenazas nos obligan a nuevas soluciones, algunas de las cuales ya hemos señalado, y que podrían resumirse en:

- **Tecnológicas:** basadas en aprovechar los avances tecnológicos para implementar soluciones que incidan sobre los riesgos y optimicen costes.

- **Digitalización:** Obtención, recopilación y tratamiento del dato para la toma de decisiones. Permite conocer la situación en tiempo real y justificar las decisiones adoptadas.

- **Normalización:** Tendencia a certificación bajo estándares. Cada vez es más común el obtener certificaciones en normas internacionales; esto beneficia a la empresa y garantiza un determinado nivel de cumplimiento frente al estándar. Cobra aquí especial relevancia la del profesional de la gestión de la seguridad como experto que asesora en temas de consultoría y capaz de auditar competentemente tanto de forma interna como externa en las compañías; interesante figura, además como asesor externo de compañías sin departamento de seguridad o como figura “implant” en departamentos con pocos recursos humanos propios.

- **Inteligencia, análisis, prospectiva:** Se busca una seguridad predictiva frente a la tradicional seguridad “forense”. Buscamos la anticipación para la mejor gestión de riesgos entendidos de una forma global y poder contribuir al negocio.

- **Seguridad Integral:** todo ello bajo el enfoque de la convergencia de las seguridades en una única Seguridad, basada en el director de seguridad como figura fundamental que lidera y en el departamento de seguridad como eje fundamental de la gestión y el cambio, haciendo que la seguridad pase a ser un proceso estratégico para las compañías, bajo estándares y regidos por la eficacia y eficiencia en la consecución de resultados y totalmente alineados con los objetivos empresariales.

AUTOR: José Ignacio Olmos Casado. RENFE

El concepto de seguridad, y por ende el de su departamento, está en evolución continua

Podemos hablar de que el concepto de seguridad, y por ende el de su departamento, está en evolución continua; así, podemos señalar diferentes fases:

- En un primer momento podemos hablar de una **seguridad subjetiva,** en la que la seguridad es básicamente un producto. Es una seguridad eminentemente disuasoria, con vigilantes armados y predominio de las medidas de seguridad físicas, y muy centrada en una relación exhaustiva de amenazas.

- En un segundo momento, en el que nos encontraríamos en la actualidad de forma mayoritaria, hablamos de una **seguridad tecnológica,** en la que la seguridad se constituye como un departamento más. Es una seguridad marcada por la aparición de las TIC; se desarrollan de forma vertiginosa el hardware y el software. Es una seguridad en la que se implementan los sistemas de control de accesos, videograbaciones, etc., y hay abundancia de información; al mismo tiempo la seguridad sigue siendo disuasoria y supervisada desde centros de control.

- El escalón final, al que se debería tender, es aquel compuesto por una **seguridad organizativa**, en la que la seguridad se constituye como un proceso. Aquí, la seguridad forma parte de la dirección estratégica, que es siempre lo ideal. La seguridad se gestiona y se establecen objetivos. Aparecen los sistemas de gestión y esa gestión se ejecuta contra estándares. Existen indicadores de seguridad que pueden ser revisables por la alta dirección.

Así pues, hay dos principales enfoques de la seguridad: **administrar frente a gestionar**. La mera administración no necesita de figuras especializadas, pero no aporta ningún valor a la organización. El ámbito de la gestión, sin embargo, hace referencia a llevar adelante una iniciativa o proyecto, e implica **planificar, desarrollar, controlar y actuar.**

La ley 5/2014, de 4 de abril, de seguridad privada (LSP) abordó hace casi una década una insuficiencia regulatoria que afectaba a un sector ya profesionalizado. Esta escasez jurídica era especialmente patente en lo que se refería a la actividad de la investigación privada y a los detectives privados.

El propio prólogo de la LSP expone que *"esta ley afronta de manera decidida y completa, en lo que le corresponde, la definición de su contenido, perfiles, limitaciones y características de quienes, convenientemente formados y habilitados, la desarrollan. De esta manera* ***la regulación de las actividades y el personal de investigación privada pasa a constituir uno de los elementos fundamentales de la nueva ley****, abandonando la presencia colateral que tiene en la vigente normativa."*

El artículo 2 enmarca dentro del concepto amplio de seguridad privada al *" conjunto de actividades, servicios, funciones (...) realizadas o prestados por (...)* ***despachos de detectives privados*** *(…) para realizar averiguaciones sobre personas y bienes, con la finalidad de* ***garantizar la seguridad de las personas, proteger su patrimonio y velar por el normal desarrollo de sus actividades."*** En el mismo artículo se define a los despachos de detectives privados como *" las oficinas constituidas por uno o más detectives privados que prestan servicios de investigación privada."*

Los servicios de investigación privada cubren una serie de necesidades de información y de obtención de pruebas relativas a hechos privados que afectan a terceros que ostentan un interés legítimo sobre los mismos en el ámbito económico, laboral, mercantil, financiero, familiar, social, etc.

Para el desarrollo de estos servicios, los detectives privados se convierten en "**buscadores y observadores**" que recopilan datos e informaciones de una amplia variedad de fuentes (humanas, registrales, abiertas, etc.). En este camino, frecuentemente, el detective se cruza con hechos, informaciones y datos que afectan a la seguridad pública.

Más allá que lo que determina el consabido artículo 14 de la LSP, la colaboración de los detectives privados con los cuerpos policiales se asienta en la implicación del profesional en contribuir al bienestar público.

Esta implicación se materializa en la comunicación de cualquier circunstancia o información relevante para la prevención, el mantenimiento o restablecimiento de la seguridad ciudadana, así como todo hecho delictivo del que tuviesen conocimiento a las Fuerzas y Cuerpos de Seguridad.

Para llevar a cabo esta relación de colaboración con la Policía Nacional, el profesional de la investigación tiene diferentes opciones que van desde personarse en una dependencia policial para poner en conocimiento los hechos, informar a la Unidad Territorial de Seguridad Privada (UTSP) de la demarcación o través de la Sección Operativa de Colaboración de la Unidad Central de Seguridad Privada (UCSP). En este sentido, es de subrayar el **canal bidireccional de comunicación RED AZUL,** que facilita la aportación de informaciones a través de la propia página web o través del correo **redazul@policia.es,** lo cual aporta grandes ventajas, entre las que podemos mencionar la inmediatez en la recepción de la información y su conexión únicamente con el número de RNSP o la TIP. Esto último evita que, en el tratamiento posterior que se haga de esa información en otras dependencias policiales que no sean la UCSP o las UTSP, la misma lleve asociada otros datos del detective, los cuales solo se aportarían en el supuesto de que la unidad policial concreta que vaya a explotar la información así lo solicite a la UCSP o UTSP por ser necesario en su investigación policial.

No obstante, esa comunicación telemática que, por un lado facilita la colaboración, a veces, por desconocimiento, puede dar lugar a pensar que la información queda "guardada en un cajón". Nada más lejos de la realidad. Si el lector de estas líneas se está preguntando si esas comunicaciones sirven para algo la respuesta es SÍ.

La información una vez recibida en RED AZUL, es analizada y tratada por el grupo operativo de la UCSP encargado de su análisis y tratamiento, el cual lleva a cabo las gestiones necesarias para integrarla en el ciclo de inteligencia y poder ser utilizada por cualquier unidad policial operativa. Si la información diera lugar, desde su origen, a una actuación policial concreta, además de lo anterior, se enviaría directamente a la dependencia policial competente.

Durante 2022, el 70 % de la inteligencia aportada por el sector de la seguridad privada provino de detectives privados, quedando patente con ello **la aportación que los investigadores privados de este país hacen a conseguir entornos seguros, garantizar la convivencia y a generar valor público.**

Puede ser que el título del presente artículo provoque en el lector reacciones muy distintas, dependiendo del conocimiento normativo y del bagaje profesional del que disponga.

En muchas ocasiones, de forma coloquial, y por personas con escasos conocimientos normativos, se denomina a la persona que realiza un control de accesos como *"el de seguridad",* infiriéndole misiones y funciones propias de los profesionales de la seguridad privada. En esa misma línea, no nos resulta extraño cuando conversamos con un conocido, familiar o amigo, que el mismo nos manifieste que ha estado en un determinado evento (concierto, festival, exposición, por ejemplo) y se refiera al controlador de accesos de la misma forma.

Este error de concepto, en la mayoría de las ocasiones, no tiene mucha repercusión porque nuestro interlocutor no tiene ningún tipo de relación con el sector de la seguridad pero sí que muestra el desconocimiento de una parte de la ciudadanía de lo que es el sector de la seguridad privada, sus profesiones y misiones.

A *sensu* contrario, alguien que tenga ciertos conocimientos sobre esta materia puede afirmar que el control de accesos no tiene nada que ver con la seguridad privada, lo cual es, en principio cierto, pero matizable.

...extender el conocimiento entre los ciudadanos de lo que es y de lo que no es la seguridad privada...

En estas líneas, de manera directa, clara y concisa se pretende aclarar ciertos aspectos y ayudar de cierta manera a extender el conocimiento entre los ciudadanos de lo **que es y de lo que no es la seguridad privada,** describiéndose conceptos harto sencillos para los expertos de seguridad privada pero, desconocidos para el grueso de la ciudadanía.

La ley de seguridad privada (LSP), Ley 5/2014, determina en su articulado las actividades de seguridad privada que, resumidamente, son las siguientes:

a) La vigilancia y protección de bienes, establecimientos, lugares y eventos, y de las que allí se encontrasen.

b) El acompañamiento, defensa y protección de personas físicas (escoltas).

c) El depósito, custodia, recuento y clasificación de monedas y billetes y, en general, objetos valiosos.

d) El depósito y custodia de explosivos, armas, cartuchería metálica y objetos que, por su peligrosidad, precisen de vigilancia y protección especial.

e) El transporte y distribución de los objetos a que se refieren los dos párrafos anteriores.

f) La instalación y mantenimiento de aparatos y dispositivos de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia.

g) La explotación de centrales de alarmas, monitorización de sus señales y su comunicación a las Fuerzas y Cuerpos de Seguridad competentes en estos casos.

h) La investigación privada en relación a personas, hechos o delitos sólo perseguibles a instancia de parte.

Los servicios sobre las actividades relacionadas sólo podrán prestarse por empresas de seguridad privada, excepto la investigación privada, que es propia de los despachos de detectives de forma exclusiva y excluyente.

Por otro lado, la LSP detalla determinadas **actividades compatibles, que no son exclusivas de seguridad privada** pero que sí se desarrollan en multitud de ocasiones en entornos muy próximos o junto a los servicios de seguridad, encontrándonos ahí el tan conocido **control de accesos:** información o control en los accesos a instalaciones realizado por porteros, conserjes y demás personal auxiliar análogo. Esta actividad, por tanto, **queda fuera del ámbito exclusivo de la seguridad privada,** primer concepto que se quiere plasmar en estas líneas, pudiendo ser realizado por empresas y personal ajeno a la seguridad privada.

Aclarado este primer aspecto, enseguida surge una pregunta: ¿puede hacer un control de accesos personal de seguridad privada, concretamente, el vigilante de seguridad? **La respuesta es SÍ.** Un vigilante de seguridad, siempre con carácter complementario y sin que en ningún caso constituyan el objeto principal del servicio que preste. Es decir, y a modo de resumen, el control de accesos puede ser realizado tanto por personal ajeno a la seguridad privada como personal habilitado.

...debemos distinguir dos tipos principales de controles de accesos fuera del ámbito de la seguridad privada...

Llegados a este punto, debemos distinguir dos tipos principales de controles de accesos fuera del ámbito de la seguridad privada: el control de accesos de un edificio, recinto o entidad, pública o privada, los conocidos coloquialmente como conserjes, que sus funciones vienen reguladas en sus contratos laborales, sin poder realizar en ningún caso actividades exclusivas de seguridad privada, y por otra parte, el control de accesos en espectáculos públicos y actividades recreativas, los cuales se rigen por una normativa propia con ámbito competencial de las Comunidades Autónomas, las cuales pueden legislar dicha actividad en su territorio, teniendo la competencia para exigir, si así lo estiman necesario, una titulación específica para poder llevar a cabo esta actividad dentro de su ámbito territorial.

Un ejemplo es la Comunidad de Madrid, la cual mediante la Ley 17/1997, de 4 de julio, de Espectáculos Públicos y Actividades Recreativas, y su posterior desarrollo en el Decreto 163/2008, de 29 de diciembre, por el que se regula la actividad de control de acceso a Espectáculos Públicos y Actividades Recreativas, especifica las funciones que podrán desarrollar el personal de control de acceso, así como los requisitos necesarios para poder ejercer esta trabajo, siendo uno de ellos el haber superado en la Academia de Policía Local de la Comunidad de Madrid, actualmente denominado Instituto de Formación Integral en Seguridad y Emergencias (IFISE), las pruebas correspondientes para al obtención del certificado acreditativo para desarrollar estas funciones, el cual tiene una validez de cinco años desde el momento de su expedición, siendo necesaria su renovación para seguir desarrollando estos puestos de trabajo.

Dicha regulación propia especifica, a su vez, la obligatoriedad de portar de forma visible y permanente un distintivo que le identifique y le acredite como tal, correspondiendo a los Ayuntamientos el ejercicio de las funciones inspectoras que garanticen el cumplimiento de las referidas normas, además de la propia Comunidad de Madrid en el ámbito de sus competencias. Dichas inspecciones podrán ser realizadas por funcionarios de las Fuerzas y Cuerpos de Seguridad del Estado, de las Policías Locales o por funcionarios de la Comunidad de Madrid y de los Ayuntamientos debidamente acreditados.

Quizá, como consecuencia de lo descrito hasta el momento, se podría pensar que la LSP es ajena a las empresas y personas que realizan el control de accesos y debería ser así pero, desgraciadamente, el desconocimiento, en unos casos, y la mala praxis, en otros, hacen que es la LSP no sea ajena al control de acceso, ya que la labor inspectora y el régimen sancionador de la misma es aplicable a aquellas empresas que presten servicios de seguridad privada sin estar autorizadas para ello y a las personas que ejerzan estas funciones sin estar habilitadas para ello. Es decir, empresas que no son empresas de seguridad, y personal que no es personal de seguridad privada.

Esta transgresión de la norma puede conllevar sanción para tres sujetos distintos: la empresa de control de accesos, el controlador de accesos y la empresa usuaria o cliente...

Por tanto, la LSP es aplicable al control de accesos cuando, a la hora de llevar a cabo el mismo, se exceden las funciones propias extendiéndolas a aquellas que solo pueden realizar las empresas de seguridad y el personal habilitado, que no es otra cosa que **intrusismo**. Esta transgresión a la norma puede conllevar sanción para tres sujetos distintos: la empresa de control de accesos, el controlador de accesos y la empresa usuaria o cliente, la cual ha contratado para desarrollar el servicio de seguridad a una empresa que no puede realizarlo.

Justificar el desconocimiento o una negligencia excusable a una empresa de control de accesos que ha sido propuesta para sanción por intrusismo, desde el punto de vista de los organismos competentes y de los profesionales del sector de la seguridad privada, es harto difícil. Una empresa que se dedica a una determinada actividad debe conocerla a la perfección y, sobre todo, conocer los límites de la misma. En supuestos muy puntuales y concretos podría ser entendible, **pero nunca justificable,** la mala praxis de una empresa de servicios.

En lo que se refiere a las personas que llevan a cabo el control de accesos, la casuística es algo más variada, abarcando el espectro desde personas con

necesidades económicas que son "colocadas" para llevar a cabo dicha función y que, en multitud de ocasiones, no sólo carecen de la habilitación de seguridad privada, si no también de la consiguiente titulación autonómica para llevar a cabo exclusivamente el control de accesos, estando completamente ausentes de lo que es el sector de la seguridad privada; hasta personas que, sabiendo perfectamente que están trasgrediendo lo establecido legalmente, tratan de enmascarar su actuación con ambigüedades e incongruencias cuando son sorprendidos haciendo intrusismo. En este último caso sí que nos encontramos a controladores titulados que se exceden en sus funciones, normalmente, por indicación de la empresa de servicios a la que pertenecen.

Por último, están los usuarios o clientes. Dado el carácter divulgativo que tienen estas líneas, es en este tercer eslabón de la cadena sobre el que se quiere incidir, pues no es ajeno, ni mucho menos, al régimen sancionador de la LSP.

Sin querer hacer una justificación jurídica ni legal, *ignorantia juris non excusat* (la ignorancia de la ley no es excusa de su cumplimiento) es un principio del Derecho del que mucho se ha escrito y que ha sido referenciado en sentencias judiciales de los diferentes ámbitos, y del que deben hacerse eco todas aquellas personas, físicas o jurídicas, que vayan a contratar un determinado servicio para un control de accesos, **debiendo tener claro cual es su necesidad, qué tipo de empresa debe contratar y que tipo de profesional debe desarrollar el servicio**. No preocuparse o no asesorarse por conocer la regulación básica de un determinado sector puede hacer, en el caso de la seguridad privada, ser propuesto para sanción.

Aparte del desconocimiento, a veces real, a veces simulado, que alegan algunas personas cuando se les propone para sanción por transgredir la normativa de seguridad privada, existen casos en los que la motivación es económica, buscando ahorrar costes, para lo cual se camuflan servicios de seguridad bajo la apariencia de ser "simplemente" un control de accesos.

También se da el supuesto de que el usuario/cliente, no contrata a empresas de servicios para llevar a cabo ese servicio de seguridad encubierto bajo la denominación de control de accesos, si no que utiliza a sus propios trabajadores, convirtiéndose el cliente en empresa intrusa, siendo propuesto para sanción por ello.

Para finalizar con este "tercer eslabón", se quieren mencionar los supuestos en los que los usuarios o clientes de una empresa y/o personal intruso lo son por haber sido amenazados por los mismos de una manera velada, obligándoles a contratar sus servicios apoyados en el miedo que infunden mediante unas sugerencias que esconden verdaderas extorsiones a las que no se debe acceder, y que deben ser puestas en conocimiento de los cuerpos policiales competentes para su investigación y enjuiciamiento.

Durante el año 2022 la Policía Nacional ha elevado un total de 337 propuestas de sanción a empresas y personal intruso, así como a usuarios de los mismos.

Con un objetivo completamente informativo, se quiere hacer constar que, durante el año 2022, la Policía Nacional, a través de su Unidad Central de Seguridad Privada (Autoridad Nacional de Control) y las Unidades Territoriales, han elevado un total 337 propuestas de sanción a empresas y personal intruso, así como a usuarios de los mismos.

RIESGOS POTENCIALES DEL USO DE LA INTELIGENCIA ARTIFICIAL A TRAVÉS DEL CHATGPT

De manera oficial, en la actualidad no hay información disponible sobre si tecnologías como ChatGPT son utilizadas o pueden estar vinculados a formas de delincuencia organizada, existendo el riesgo de que los chatbots, basados en el procesamiento del lenguaje natural, como es el caso de ChatGPT, podrían usarse para mejorar ciertas formas de ciberdelincuencia.

Un estudio conjunto realizado por United Nations Interregional Crime and Justice Research Institute (UNICRI) y el Centro Europeo de Ciberdelincuencia de Europol nos proporciona detalles sobre las posibles amenazas que plantean Inteligencia Artificial (AI). Por parte de estas entidades se han identificado algunos riesgos específicos que se detallan, a continuación:

- **Mayor riesgo de ataques de phishing**, pudiendo aumentar el riesgo de este tipo de ataques. Los ciberdelincuentes podrían usar ChatGPT para interactuar con los usuarios y engañar para que revelen información confidencial, como son las credenciales de inicio de sesión o información financiera. El sistema de IA también podría usarse para hacerse pasar por negocios legítimos o personas, lo que dificulta que los usuarios distingan entre una solicitud genuina y una falso.

- **Riesgo de desinformación amplificada,** la disponibilidad pública de ChatGPT hace que se aumente el riesgo de desinformación generalizada, ya que el sistema de IA podría usarse para difundir información falsa o propaganda a gran escala, lo que puede conducir a un daño significativo. La capacidad del sistema generar contenido convincente y persuasivo podría dificultar que los usuarios distinguir entre lo que es verdadero y lo que es falso, lo que genera confusión y desconfianza.

- **Desarrollo potencial de nuevos métodos de ataque**, La disponibilidad de ChatGPT para el público también supone un riesgo de uso malicioso por parte de los ciberdelincuentes. Hackers y otros actores maliciosos podrían potencialmente usar el sistema de IA para desarrollar nuevos métodos y herramientas de ataque. ChatGPT podría usarse para generar correos electrónicos de phishing convincentes o malware que puede evadir los métodos de detección tradicionales. Además, el sistema de IA tiene la capacidad de adaptarse y aprender, y podría dar lugar a la creación de nuevo malware creado por IA que tiene una firma completamente diferente. Esta capacidad de autoaprendizaje podría dificultar medidas de seguridad para mantenerse al día con las amenazas emergentes.

- **Mayores preocupaciones sobre la privacidad**, ya que el sistema de IA está diseñado para aprender y adaptarse a partir de las interacciones de los usuarios, planteando preguntas sobre cuántos datos se recopilan y cómo se utilizan. Los usuarios también pueden estar preocupados por la posibilidad de que sus conversaciones con ChatGPT sean almacenadas y analizadas por terceros sin su conocimiento o consentimiento.

Con todo lo anterior se podrían destacar diferentes escenarios de riesgo clave, siendo los siguientes algunos ejemplos de actividad delictiva por parte de personas que utlizaran la IA:

- Adivinación de contraseñas compatible con IA.
- Cifrado asistido por IA.
- Ingeniería Social a Escala.
- Suplantación de identidad humana en plataformas de redes sociales.
- Automatización de ataque.
- Mayor precisión en los ataques.
- Mejor evasión de detección.
- Ataques personalizados.
- Fraude y usurpación de identidad.

Desde Europol avisan que esta lista preliminar no es exhaustiva y que los riesgos adicionales en el campo de la ciberdelincuencia, así como en otras áreas delictivas, podrían surgir aún más si cabe con el uso de esta herramienta y de otras relacionadas con la IA, especialmente si los grupos criminales entrenaran sus propios modelos sin la restricción de la moral, que es

la política de contenido actualmente configurada por los creadores de ChatGPT.

La prevención de la ciberdelincuencia en la era de la IA es un desafío importante. Los sistemas de seguridad tradicionales pueden no ser suficientes para protegerse de los ataques de los ciberdelincuentes por lo que se deberían utilizar sistemas de seguridad avanzados.

Algunos consejos a tener en cuenta:

- Utilice contraseñas seguras (combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales).
- Utilice autenticación de dos factores.
- Asegúrese de mantener un software actualizado.
- No hacer clic en enlaces sospechosos.
- Usar software antivirus.
- Hacer copias de seguridad de los datos.
- Ser cauteloso al compartir información personal.

Desde Europol se anima a todas las instituciones a compartir cualquier información pertinente sobre cualquier actividad delictiva detectada relacionada con este fenómeno.

EL 'TIMO DEL AMOR', EL CIBERDELITO CON EL QUE HAN ESTAFADO MÁS DE UN MILLÓN DE EUROS EN ESPAÑA

Esta nueva forma de relacionarse a través de las redes sociales también es utilizada por los ciberdelincuentes para cometer estafas. Recientemente la Policía Nacional desarticuló a un grupo de 18 personas que creaba perfiles falsos y que llegó a estafar más de un millón de euros a 90 individuos en España.

Los detenidos recurrían al **'timo del amor'**, es decir, empleaban "todo tipo de artimañas" para conseguir que sus víctimas se enamorasen y accediesen a darles dinero. Los ciberdelincuentes trataban de ganarse la confianza de sus víctimas para luego enviar un supuesto regalo que terminaba siendo retenido en aduanas o por una empresa de transporte y, para liberarlo, pedían cantidades "desproporcionadas" de dinero. En algunos casos incluso, se llegaba a amenazar a las víctimas si no realizaban los pagos, lo que ocasionaba "un miedo insuperable" y que terminasen haciéndolo.

En cuanto las víctimas dan el dinero, los delincuentes las bloquean.

Consejos para no caer en la trampa

- **Asegúrate de que la persona al otro lado de la pantalla es real** y que no está sumplantando una identidad.
- **No enviar dinero a personas que no se conocen en la vida real.**
- **No contar información confidencial** ni enviar imágenes o vídeos comprometidos a extraños ya que pueden utilizarlo para posteriores extorsiones.
- En caso de ser víctima debe **denunciarse** el hecho.

EL RIESGO DE COMPARTIR EL NÚMERO DE CUENTA

Para realizar alguna compra online, en algún trámite con las administraciones pública, o en otras operaciones que realizamos de manera telemática, lo normal es que nos soliciten el número de nuestra cuenta bancaria, el cual facilitamos para poder llevar a cabo una gestión personal una manera rápida, pero **¿sabemos que podría hacer un delincuente con ese dato?**

Inicialmente, con ese único dato, el cual es confidencial, una persona ajena no puede extraer dinero de nuestra cuenta. Ahora bien, si además de conocer el número de nuestra cuenta, esa persona desconocida dispone del número de nuestro DNI, en algunos casos podrá realizar una domiciliación de recibos en nuestra cuenta. En estos casos, si hubiera algún movimiento no permitido, la solución es fácil y rápida, al poder devolver sin problemas el recibo correspondiente, siempre y cuando tengamos un control periódico y regular sobre nuestros movimientos en cuenta.

Otra cosa sería que un tercero disponga de tu número de tarjeta de débito o crédito y quiera hacer un mal uso de esta, ya que puede realizar movimientos de dinero, haciendo que seamos víctimas de un fraude.

En estos casos, desde el Banco de España nos aconsejan tomar las siguientes medidas de seguridad:

- No anotar ni llevar escrito el pin en un papel.
- Toma medidas de confidencialidad en los cajeros, es decir, que nadie te vea marcar el pin.
- Comprobar los extractos del banco para detectar movimientos sospechosos.
- No utilizar la tarjeta de crédito como identificación personal.
- Si usas la tarjeta para comprar en Internet, utilizar al menos tres de las medidas de seguridad.
- No facilitar datos clave de tu tarjeta para el pago de forma telemática (por teléfono, por internet, etc.), a menos que sean personas o en sitios web de total confianza.

BUSINESS EMAIL COMPROMISE (BEC): CIBERFRAUDE A LAS EMPRESAS

La reciente desarticulación por la Policía Nacional de una organización criminal dedicada a esta modalidad delictiva ha puesto de manifiesto la necesidad de hacer un somero recuerdo de en qué consiste el *BEC (Business Email Compromise)*.

En el *BEC* el ciberdelincuente consigue entrar en el correo empresarial de alguien que ocupa un puesto de cierta relevancia o con competencias en realización de pagos. El acceso a la cuenta de correo se realiza mediante técnicas de ingeniería social o través de un email de phising.

Una vez que el delincuente tiene acceso a la agenda de contactos, selecciona el contacto de un proveedor de dicha empresa y suplanta su identidad, enviando un correo informando de un cambio en la cuenta bancaria del proveedor al que la empresa debe realizar un pago por un servicio prestado, por la provisión de un determinado tipo de producto, etc. El estafador normalmente ha realizado un estudio de la información de la cuenta de correo (contactos frecuentes, operaciones comerciales pendientes, etc.) y se ha hecho pasar por un proveedor al que se le va a realizar un pago en próximas fechas.

El pagador realiza el ingreso en la nueva cuenta bancaria que le han facilitado, sin sospechar que realmente lo está haciendo en una que no es de su proveedor habitual, sino que está a nombre de una "mula" (colaborador) del cibercriminal.

¡¡¡ OJO, NUEVA MODALIDAD DE *SPOOFING* !!!

El ***spoofing*** consiste en la **suplantación del número de teléfono real** de compañías energéticas, entidades bancarias o instituciones públicas, que unido a técnicas de ingeniería social, hacen que sea **una estafa casi indetectable.**

Si bien el *spoofing* no conforma un método de estafa novedoso como tal, los especialistas en la lucha contra la ciberdelincuencia de la Policía Nacional han detectado un perfeccionamiento de la técnica que hace más difícil su detección por parte de las víctimas:

1. Los ciberdelincuentes **suplantan el número de teléfono real** de tal forma que si la víctima comprueba a quién pertenece dicho número verá que, efectivamente, se trata de la empresa o entidad a la que los estafadores están suplantando.

2. En la conversación telefónica se ganan la confianza de sus víctimas hablando sobre cuestiones de seguridad de su cuenta, **advirtiéndoles que no verbalicen las claves.**

3. Seguidamente, y alegando falsos motivos de seguridad, **les indican que marquen en el teclado de su terminal móvil la clave de acceso** a la banca privada, o un código de verificación, a través de un enlace remitido en ese mismo momento por sms.

4. **Los estafadores captan las pulsaciones que teclea en el móvil** y pasan a controlar sus claves secretas.

RECOMENDACIONES:

- **No aportar nunca datos** personales ni bancarios **sin cerciorarse** de que se trata de la empresa o entidad en cuestión.
- Recordar que **ninguna empresa privada o institución pública** utiliza este método para **solicitar datos de carácter personal a sus clientes.**
- **No facilitar nunca información** de tarjetas, documentos de identidad, declaración de la renta, nóminas, nombres de usuario, claves y contraseñas.
- **No aceptar en ningún caso, las condiciones que ofrezcan en una misma llamada o comunicación**. Solicitar que nos remitan la documentación para su estudio o emplazar a que nos realicen una segunda llamada para que podamos hacer comprobaciones.
- **No clicar en los enlaces de los mensajes de texto que nos envíen** y en el caso de cuentas bancarias, acceder siempre a través de la aplicación que nos facilitan las entidades financieras, compañías telefónicas o empresas de suministro.

ROBOS CON FUERZA EN VIVIENDAS

Como cada año por estas fechas, todos empezamos a pensar en las vacaciones de verano, mirando lugares que queremos visitar, reservando medios de transporte y alojamientos e iniciamos nuestra particular cuenta atrás ansiando el día de inicio de nuestro descanso estival.

Este entusiasmo ante la llegada de nuestras ansiadas vacaciones hace que, a veces, no pensemos en lo que dejaremos durante ese periodo: nuestra vivienda. Igual que planificamos nuestro ocio veraniego, debemos pensar en dejar lo más protegido nuestro hogar para tratar de evitar disgustos y frustraciones al regresar de las vacaciones.

Un año más, y con el objetivo de reducir las posibilidades de que nuestra casa sea objeto de un robo, se recuerdan una medidas preventivas, **invitando a todos los profesionales del sector a que las difundan** entre su familiares, personas allegadas y de su entorno laboral y personal.

Siempre hay que asegurarse que todas las **puertas y ventanas queden cerradas y con llave**, especialmente las que dan al exterior.

Medidas preventivas básicas

Otra medida de seguridad importante es **no dar información sobre nuestra ausencia, ya sea en lugares públicos o en las redes sociales.** Nunca sabemos quién nos está escuchando o si los ladrones espían nuestras publicaciones en redes sociales.

Es de gran ayuda contar con la **colaboración de vecinos, familiares o amigos de confianza**. Podemos pedirles que revisen nuestra vivienda de vez en cuando y que recojan el correo y los paquetes que lleguen a nuestra casa para que no se acumulen y den señales de que no estamos en casa. Es de interés dejarles un número de teléfono de contacto en caso de emergencia.

Si vamos a estar fuera de casa por un periodo de tiempo prolongado, es aconsejable **dejar la casa con una apariencia de que aún estamos presentes**. Esto incluye dejar algunas luces encendidas, utilizar temporizadores, programar la televisión o la radio para que se enciendan y apaguen en distintos horarios, y dejar algún coche en el garaje. Todo esto dará la impresión de que hay alguien en casa y puede disuadir a los ladrones.

¡¡ Avise a la Policía si ve objetos o marcas en cerraduras o entre el marco y la puerta !!

Medidas de seguridad en los accesos

Es **recomendable la instalación de sistemas de seguridad** como alarmas, cámaras de seguridad, y sensores de movimiento. Las cámaras de seguridad es conveniente que sean instaladas en plano horizontal y en lugares con buena iluminación

Asegúrese de que todas las puertas y ventanas de su vivienda estén cerradas con **cerraduras de alta calidad** y en buen estado.

Considere la posibilidad de **instalar cierres adicionales,** sobre todo en ventanas de tipo deslizante, como cerrojos o barras de seguridad, para aumentar la seguridad. Las ventanas más seguras son las de tipo oscilo-batientes. Por otro lado los escudos protectores en la cerradura esconden la marca del bombín y la protegen. Los muelles recuperadores y retenedores aseguran que las puertas de acceso se cierran correctamente. Son recomendables los bombines precortados o antibamping y utilice productos con calidad certificada.

Las llaves en los ascensores hacen más seguro el acceso a los trasteros.

PREGUNTAS FRECUENTES

INSTALACIÓN DE SISTEMAS DE CCTV EN COMUNIDADES DE PROPIETARIOS

Consulta sobre obligación de comunicación al Mº del Interior de contratos de instalación de sistemas de CCTV en garajes y portales de comunidades de propietarios, sin previsión de conectarlas a CRA o a CCTV, con la siguiente respuesta:

Las empresas de seguridad están obilgadas a comunicar al Mº del Interior y, en su caso, órganos correspondientes de las Comunidades Autonómicas, de los contratos de los servicios de seguridad a sus clientes, recogido en el artículo 9 de la Ley 5/2014, de Seguridad Privada (LSP), que dispone en sus apartados 1 y 2:

"1. No podrá prestarse ningún tipo de servicio de seguridad privada que no haya sido previamente contratado y, en su caso, autorizado.

2. De acuerdo con lo que reglamentariamente se determine, los contratos de prestación de los distintos servicios de seguridad privada deberán, en todo caso, formalizarse por escrito y comunicarse su celebración al Ministerio del Interior o, en su caso, al órgano autonómico competente con antelación a la iniciación de los mismos".

Los servicios que deban ser comunicados por estas empresas, deberan atender a lo dispuesto en los artículos 5.1.f) y 46.1 de la LSP, que establecen lo siguiente:

El artículo 5.1, f, define la actividad como: "instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia.

El artículo 46, en relación con el servicio de dicha actividad, dispone:

"1. Los servicios de instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, consistirán en la ejecución, por técnicos acreditados, de todas aquellas operaciones de instalación y mantenimiento de dichos aparatos, equipos, dispositivos o sistemas, que resulten necesarias para su correcto funcionamiento y el buen cumplimiento de su finalidad, previa elaboración, por ingenieros acreditados, del preceptivo proyecto de instalación, cuyas características se determinarán reglamentariamente.

Así mismo, es preciso tener presente lo dispuesto por el artículo 42.1 de la LSP, al tratarse de instalación de cámaras, donde se establece lo siguiente:

"1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.

No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del 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. Estas funciones podrán realizarse por personal distinto del de seguridad privada".

Conclusiones: Las empresas inscritas en el Registro Nacional de Seguridad Privada, para el desarrollo de la actividad del artículo 5.1.f) de la LSP, **únicamente deberá comunicar al citado Registro Nacional o, en su caso, el Registro Autonómico correspondiente, aquellas instalaciones de aparatos, equipos, dispositivos y sistemas de seguridad que están conectados con centrales receptoras de alarmas, centros de control o de videovigilancia o, en su caso, sea una medida de seguridad impuesta por la autoridad competente.** Por lo que habrá de conocerse, con el objeto de evitar una posible sanción administrativa, que el sistema de CCTV que se alude en la consulta, y que está previsto sea instalado en varias comunidades de propietarios, que en ningún caso se conectará a una central receptora de alarmas o a un centro de videovigilancia, en este último caso, teniendo en cuenta los términos y finalidades descritas en el artículo 42.1 de la Ley 5/2014, de Seguridad Privada.

INTERLOCUTOR POLICIAL SANITARIO: NOTICIAS

LA POLICÍA NACIONAL SE REÚNE CON EL COLEGIO DE FARMACÉUTICOS DE BADAJOZ

El Interlocutor Policial Territorial Sanitario (IPTS) y jefe de la Unidad Territorial de Seguridad Privada de Badajoz se reunión con representantes del Servicio Extremeño de Salud y del Colegio de Farmacéuticos para estudiar y analizar la casuística y circunstancias de las agresiones a los profesionales de esta especialidad sanitaria, así como de los delitos contra la propiedad que sufren las farmacias en esta parte del territorio nacional.

"*PREVENCIÓN Y REACCIÓN ANTE LA AGRESIÓN EN EL ÁMBITO SANITARIO"* EN LA RIOJA

El IPTS de La Rioja y su equipo, integrantes todos ellos de la Unidad Territorial de Seguridad Privada en esta comunidad organizaron una jornada formativa dirigida a profesionales sanitarios: ***"Prevención y Reacción ante la agresión en el ámbito sanitario"***

La acción se desarrolló en dependencias del Centro de Investigación Biomédica de La Rioja (CIBIR) y su inauguración corrió a cargo de la Delegada del Gobierno en la Rioja, la Consejera de Sanidad y el Jefe Superior de Policía de La Rioja.

Los objetivos de la formación eran la difusión de información entre los profesionales sanitarios, la creación de hábitos de seguridad en sus respectivos centros de trabajo, así como la potenciación de habilidades y la dotación de herramientas que les permitan manejar de forma adecuada aquellas situaciones de elevada tensión, tratando de evitar posibles agresiones o en última instancia minimizando sus consecuencias. De igual modo, se recalcó la importancia de la denuncia como único cauce para hacer visible el problema y poder abordarlo de forma adecuada. En las ponencias, a cargo del propio IPTS, y de otros expertos policiales destinados en esta Jefatura Superior de Policía, se detallaron los recursos que la Policía Nacional pone a disposición de los sanitarios en caso de agresión, medidas preventivas básicas y la contención verbal como herramienta para control de conflictos, finalizando la jornada con unas pautas prácticas de reacción ante la agresión mediante la escenificación de situaciones reales centradas en la evasión del profesional sanitario ante hechos violentos. La jornada contó con la asistencia de 35 profesionales sanitarios.

EL JEFE DE LA UCSP EN LA CELEBRACIÓN DEL DÍA MUNDIAL DE LA SEGURIDAD Y SALUD EN EL TRABAJO

El día 28 de abril se celebró el día mundial de la seguridad y salud en el trabajo, llevándose a cabo una formación en el Hospital Universitario 12 de Octubre en la que participó el jefe de la UCSP e Interlocutor Policial Nacional Sanitario en las que se recordó como un sanitario puede evitar una agresión.

INTERLOCUTOR POLICIAL SANITARIO: NOTICIAS

JORNADA FORMATIVA EN ASTURIAS

En la Jefatura Superior de Policía de Asturias la Interlocutora Policial Sanitaria y jefa de la UTSP impartió una jornada formativa sobre las técnicas y herramientas de prevención ante las agresiones de personal sanitario.

En dicha jornada se dio a conocer la situación actual de las agresiones en el Área Sanitaria III del SESPA, el ámbito penal y policial de las agresiones a profesionales sanitarios y las principales técnicas y herramientas de prevención ante dichas agresiones.

LA POLICÍA NACIONAL EN LAS FACULTADES UNIVERSITARIAS SANITARIAS DE EXTREMADURA

El jefe de la UTSP de Badajoz e IPTS de dicha provincia ha iniciado una colaboración docente en los cursos programados por la Consejería de Sanidad y Servicios Sociales, dirigidos a alumnos de las Facultades y Escuelas de Medicina, Enfermería y Fisioterapia de Badajoz, Cáceres, Mérida y Plasencia.

El objetivo es concienciar y sensibilizar a los futuros sanitarios sobre el papel fundamental de las medidas policiales a adoptar frente a agresiones a profesionales de la salud y la importancia del Plan de Prevención, Actuación y Atención a Personal Sanitario Público de Extremadura, fruto de la colaboración con la Consejería de Sanidad y Servicios Sociales de la región.

Se tratarán las medidas, acciones y actividades en materia de prevención de la violencia externa y el procedimiento de actuación común ante cualquier tipo de agresión o intimidación. También se analizarán los casos en que, una vez producido el acto de agresión al profesional, se pueda garantizar a la persona afectada su acompañamiento, asistencia y asesoramiento en todo momento hasta que finalice el proceso.

JORNADA EUROPEA DE AGRESIONES AL PERSONAL SANITARIO

En esta jornada se presentaron los datos de las agresiones al colectivo médico en el año 2022 en la Organización Médica Colegial (OMC) en la que participaron representantes del sector de varios países europeos. El IPNS, intervino como ponente, presentado la figura del Interlocutor Policial Sanitario y el futuro en la seguridad sanitaria.

LA POLICÍA NACIONAL EN LA CONMEMORACIÓN DEL "DÍA EUROPEO CONTRA LAS AGRESIONES A PROFESIONALES SANITARIOS" CELEBRADA POR EL MINISTERIO DE SANIDAD

El acto, llevado a cabo en la sede del Ministerio contó con la presencia del Interlocutor Policial Nacional Sanitario en una mesa redonda donde reiteró el compromiso de la Policía Nacional en la prevención y persecución de las agresiones a este colectivo.

VIII ACTO DE RECONOCIMIENTO AL MÉRITO DE LA SEGURIDAD Y PROTECCIÓN DE LA ASOCIACIÓN INTERNACIONAL DE SEGURIDAD Y PROTECCIÓN CIVIL "SAN CRISTOBAL DE MAGALLANES"

El pasado 29 de marzo tuvo lugar el acto de reconocimientos al Mérito de la Seguridad y Protección por parte de la Asociación Internacional de Seguridad y Protección Civil "San Cristóbal de Magallanes" (AISPC) presidido por el Comisario Principal, director del Centro Universitario de Formación de la Policía Nacional, el Teniente General, director de Infraestructura del Ministerio de Defensa, el Rector de la Sociedad de Estudios Internacionales y el Presidente de la AISPC.

Entre los mencionados estaba el **Comisario General de Seguridad Ciudadana,** el cual fue el encargado de dirigir unas palabras a todos los asistentes en representación de los condecorados.

JORNADA SOBRE CUESTIONES Y DUDAS EN LA APLICACIÓN DE LA NORMATIVA DE SEGURIDAD PRIVADA

El salón de actos de la Confederación de Empresarios de Málaga (CEM) acogió la celebración de una jornada organizada por AMES (Asociación Malagueña de Empresas de Seguridad) en colaboración con la Federación Empresarial Española de Seguridad.

El contenido fue impartido por el inspector, jefe del Grupo Operativo de Medidas de Seguridad, Sección Operativa de Inspección de la UCSP, que estuvo acompañado por una responsable de la Unidad Territorial de Seguridad Privada de Málaga.

Entre otros temas, se trataron los requisitos y condiciones en la prestación de servicios por las empresas de seguridad privada, las actividades de instalación y mantenimiento y vigilancia y protección y los sistemas de CCTV en las comunidades de propietarios.

Cerró la jornada el Jefe de la Unidad Central de Seguridad Privada.

JORNADA SOBRE CIBERSEGURIDAD EN MURCIA

La Unidad Territorial de Seguridad Privada de la Jefatura Superior de Policía de la Región de Murcia, por segundo año consecutivo, organizó una jornada formativa en materia de ciberseguridad, la cual se llevó a cabo en el Archivo General de la Región de Murcia, con la asistencia e inauguración de la misma por el Jefe Superior de Policía de Murcia. Entre los ponentes se contó con la Discipline Leader de seguridad de la información en BBVA y un detective privado especialista en ciberinvestigación e informática forense. Se trataron temas como la importancia de adaptar sus empresas con las medidas de seguridad informáticas necesarias para evitar aquellos delitos que se cometen mediante el uso de entornos digitales, redes, *blockchain*, computadoras, sistemas informáticos u otros dispositivos de las nuevas tecnologías de información y comunicación.

FORMACIÓN SOBRE VERIFICACIÓN OPERATIVA DE DOCUMENTOS EXTRANJEROS A INTEGRANTES DE DEPARTAMENTOS DE SEGURIDAD

Organizada por la Unidad Central de Seguridad Privada e impartida por expertos del Punto Atenas de la Comisaría General de Extranjería y Fronteras de la Policía Nacional. La formación, eminentemente práctica, se desarrolló en dos jornadas en las que integrantes de departamentos de seguridad del sector bancario adquirieron las competencias necesarias para poder realizar una verificación sobre la autenticidad o falsedad de documentos extranjeros de identidad, conducción y viaje.

COORDINACIÓN DE LA UCSP CON EMPRESAS DE VIGILANCIA Y PROTECCIÓN

Con el objetivo de afianzar y fortalecer la coordinación de la Policía Nacional con las empresas de seguridad privada que desarrollan la actividad de vigilancia y protección, la UCSP organizó una reunión de coordinación con las personas que ejercen la jefatura de seguridad y de representación de estas empresas.

Se desarrolló en las instalaciones policiales de Canillas en formato presencial y también se retransmitió en streaming con el objeto de facilitar una mayor presencia y evitar desplazamientos desde las localidades más alejadas de la capital.

Durante la misma se abordaron distintos temas, entre los que se encontraban los servicios de vigilancia discontinua, la utilización de drones en servicios de videovigilancia, la comunicación de bajas y modificaciones de contratos y la colaboración público -privada.

EL XVI CONGRESO DE DETECTIVES PRIVADOS EN PALMA DE MALLORCA

Inaugurado por la Delegada del Gobierno en Baleares junto con la presidenta del APDPE, el Comisario Provincial de Palma de Mallorca y el Jefe de la Sección Operativa de Colaboración de la UCSP.

El congreso se impartió bajo el lema “Compromiso Social” y se trataron entre otros temas la búsqueda de personas desaparecidas, la violencia sobre la mujer y menores, el detective privado en los procesos de familia y el valor probatorio de los informes de los detectives.

NOTICIAS

JORNADA EN EL ESTADIO DEL SADAR SOBRE ACTUACIONES OPERATIVAS DE SEGURIDAD PRIVADA EN ESTADIOS DE FÚTBOL

El estadio del Osasuna acogió una nueva formación dirigida a personal de seguridad privada sobre actuaciones operativas en eventos deportivos. La jornada, en el marco de la colaboración entre la Policía Nacional y LaLiga, fue organizada por la Jefatura Superior de Policía de Navarra, la Comisaría General de Seguridad Ciudadana (UCSP) y el departamento de seguridad de LaLiga. Los contenidos abarcaron desde técnicas de orden público, pasando por delitos de odio, medidas de autoprotección, las funciones de la UCO, hasta los planes de seguridad de los estadios, simbología y primeros auxilios.

LA POLICÍA NACIONAL CON LOS VIGILANTES DE SEGURIDAD DEL GRAN PREMIO DE MOTO GP EN EL CIRCUITO DE JEREZ

Un año más, el circuito de Jerez – Angel Nieto acogió la celebración del Gran Premio de Moto GP. Las características del evento y la gran afluencia de aficionados hacen necesario un dispositivo de seguridad con gran presencia de vigilantes de seguridad, cuantificándose en esta edición en 160 profesionales de la seguridad privada que se encargaron de que el Gran Premio se desarrollara sin incidencias.

En el marco del Plan Nacional de Inspección y del Plan Integral de Colaboración de la Policía Nacional con la seguridad privada (RED AZUL), integrantes de la Unidad Central de Seguridad Privada, de la Unidad Territorial de Seguridad Privada de Cádiz y de la Comisaría Local de Jerez se desplazaron al circuito para comprobar que el servicio se desarrollaba con normalidad, así como para resolver sus dudas y prestarles asesoramiento.

LA POLICÍA NACIONAL Y ORANGE COLABORAN PARA CERRAR LA BRECHA DIGITAL ENTRE LAS PERSONAS MAYORES

Dentro del marco de colaboración público-privada, la Unidad Central de Participación Ciudadana de la Comisaría General de Seguridad Ciudadana de la Policía Nacional y Orange han unido sus fuerzas para colaborar en la ayuda a las personas de más de 65 años para superar la brecha digital generacional.

Integrado dentro del **"Plan Mayor Seguridad"** se impartió el curso **"seguro con tu móvil"** en el espacio Orange Digital Center de Madrid y en otras 50 tiendas de toda España.

El curso no solo buscaba familiarizar con los medios digitales a las personas mayores, si no que también quería difundir entre los profesionales y voluntariado que velan por ellos el conocimiento de los recursos con los que cuentan para su protección y mejorar la calidad de la información sobre las telecomunicaciones.

Se recuerda que la Policía Nacional cuenta con un canal exclusivo para que la ciudadanía informe sobre cualquier situación que pueda afectar a la seguridad de nuestros mayores o a la de su entorno, así como para resolver dudas sobre el Plan Mayor Seguridad:

protegealmayor@policia.es

CELEBRACIÓN EN CANTABRIA DEL PRIMER ACTO DEL DÍA DE LA SEGURIDAD PRIVADA 2023

El primer Día de la Seguridad Privada de 2023 se celebró en Santander con el reconocimiento a la trayectoria y trabajo de 57 profesionales del sector. Un acto presidido por el Presidente de la Comunidad Autónoma acompañado de autoridades políticas y judiciales, así como de la Jefa Superior de Policía, el Jefe de la Unidad Central de Seguridad Privada y el portavoz de la Comisión de Seguridad Privada de Cantabria.

En la celebración se subrayó el **imprescindible papel de la seguridad privada en la seguridad pública.**

ISOTOPE CROSSROADS: RESPUESTA A UN INCIDENTE RADIOLÓGICO (EEUU-ESPAÑA)

La Unidad Central de Seguridad Privada de la Policía Nacional formó parte de la delegación española invitada a asistir a las jornadas ***"Isotope Crossroads",*** organizadas por la Oficina de Seguridad Radiológica del Departamento de Energía de los Estados Unidos y tuvo lugar a principios de este mes de mayo en la ciudad de San Juan, Puerto Rico.

Las citadas jornadas, en cuya organización y participación tuvo una importante colaboración el FBI, la Oficina de Seguridad Radiológica de Estados Unidos presentó un supuesto teórico de incidente con consecuencias radiológicas, concretamente un ataque por parte de un grupo criminal a un vehículo de transporte de fuente radiactiva de alta actividad, consiguiendo sustraer la misma para su posterior utilización en un lugar de concurrencia pública, ya sea como parte de un dispositivo de exposición radiológica o de dispersión radiológica (bomba sucia).

En base al escenario propuesto, las diferentes agencias participantes, en su mayoría primeros actuantes en un incidente compartieron sus procedimientos de actuación y despliegue de la respuesta adecuada. Se puso de manifiesto **la relevancia que tiene una buena coordinación y cooperación entre distintos organismos actuantes**, así como el establecimiento de una cadena de mando bien definida y planificada.

Así mismo, y como parte importante de las jornadas, la Oficina de Seguridad Radiológica mostró su interés en fortalecer sus relaciones de colaboración con España en relación a la actuación ante este tipo de incidentes.

HUELLA 2023: #UN CAMINO EN COMÚN

El Palacio de Neptuno de Madrid acogió HUELLA 2023, celebración de la publicación de los 500 números de Seguritecnia y los 100 número de Red Seguridad, reuniendo a representantes del sector público y privado de seguridad.

La Policía Nacional fue reconocida por su colaboración como ente público, así como por la difusión que desde 2018 hace de la cultura de ciberseguridad y capacitación digital mediante el Congreso C1b3RWALL. Los reconocimientos fueron recogidos por el Comisario General de Seguridad Ciudadana y un representante de la Escuela Nacional de Policía, respectivamente.

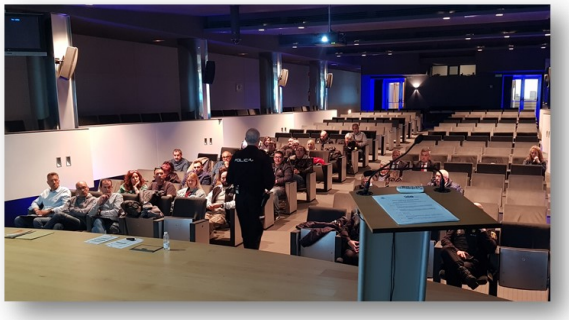
NOTICIAS

JORNADA FORMATIVA A SEGURIDAD PRIVADA EN BURGOS

El Salón Fundación Círculo de Burgos acogió la acción formativa organizada por la Comisaría Provincial de Burgos de la Policía Nacional, que iba dirigida a personal de seguridad privada. La inauguración corrió a cargo del Jefe Provincial de Operaciones de Burgos.

Los temas tratados fueron la integración de la seguridad privada en operativos dependientes de Policía Nacional, los delitos de odio, la actuación de los vigilantes de seguridad en relación a atentados terroristas y las herramientas de colaboración entre seguridad privada y pública, los cuales fueron planteados por expertos de la Comisaría Provincial y de la Unidad Central de Seguridad Privada.

Concluidas las ponencias, se abrió un turno de consultas y preguntas en las que se trataron aspectos concretos de coordinación operativa, así como de igualdad en el sector.



LA POLICÍA NACIONAL DETIENE A 11 GRAFITEROS QUE PROVOCARON 94 HECHOS DELICTIVOS EN TRENES POR VALOR DE 422.000 EUROS

Los contactos periódicos entre la Policía Nacional y las principales operadoras ferroviarias españolas permitieron llevar a cabo distintas operaciones contra grupos de grafiteros que realizaban sus pintadas en trenes y en vagones de ferrocarril y metro de distintos lugares de la geografía española.

NUEVO AVANCE EN LA INTEGRACIÓN DE LAS SEÑALES DE LAS CRA'S EN LOS CIMACC-091

En el marco del proyecto de integración de las señales de las centrales receptoras de alarmas con los CIMACC-091 de la Policía Nacional el pasado viernes, 19 de mayo, se llevaron a cabo los últimos ensayos con una de las empresas implicadas en el mismo, antes de iniciarse el periodo piloto con señales reales.

La culminación del proyecto supondrá una optimización de los recursos y un ejemplo de colaboración efectiva entre la Policía Nacional y el sector de la seguridad privada.

EL AVISO DE UN VIGILANTE EVITA EL ROBO DE VARIAS VIVIENDAS EN PALMA

El profesional de la seguridad privada se percató de la actitud sospechosa de dos jóvenes que, tras apearse de un vehículo, ocultaban sus cabezas con unas capuchas, por lo que alertó a la Policía, que acudió al lugar y procedió a la detención de los dos menores tras comprobar daños en los accesos de dos portales, un domicilio, un trastero y un bar. Se les intervino una destornillador de grandes dimensiones y una arma blanca.