

INDICATIVO

 **SIP-Añ**

SEPTIEMBRE 3/2026



ISSN: 3127-2541



INDICATIVO SUR. REVISTA OFICIAL DE SIP-AN**AÑO 2026 | NÚMERO: 003.****ISSN EN LÍNEA: 3127-2541**

Propiedad: Sindicato Independiente de Policía de Andalucía

Calle Lorenzo Cendra Busca, 6 – 29007 Málaga, CIF: G92710987,

T. 952 315 690 // Email: contacta@sip-an.es

SINDICATO INDEPENDIENTE POLICÍA DE ANDALUCÍA Comprometidos con la seguridad y el bienestar policial.

Edición, dirección y administración: SIP-AN (Sindicato Independiente de Policía de Andalucía)

Encargada de maquetación y revisión: Noemí Romero López

Guía de buenas prácticas

La revista es una publicación periódica, de ámbito andaluz, del Sindicato Independiente de Policía de Andalucía (SIP-AN).

INDICATIVO SUR tiene como objetivo difundir trabajos científicos derivados de la investigación que resulten útiles para las instituciones policiales, promoviendo el intercambio de conocimientos sobre métodos y técnicas que contribuyan a su capacitación, modernización y mejora continua.

La revista **INDICATIVO SUR** no asume responsabilidad alguna sobre el contenido de los artículos firmados por sus autores.

Ejemplar de distribución gratuita

Esta publicación digital se difunde con la colaboración del Sindicato Independiente de Policía de Andalucía. Se pondrá a disposición en la revista online de SIP-AN con el propósito de mantener actualizados y mejorar los conocimientos sobre esta materia a quienes estén interesados.

Por su relevancia en el ámbito policial, tanto su consulta como su impresión estarán accesibles para cualquier miembro de la Policía Local que desee ampliar su formación y desarrollo profesional.

© 2026 SIP-AN. Todos los derechos reservados.

Se prohíbe la reproducción total o parcial de esta obra para su inclusión en otras publicaciones sin la autorización expresa de sus autores. Se autoriza, no obstante, su impresión y difusión por cualquier medio.

Sumario

ARTÍCULOS.....	PG.5
1. Comunicación policial y desescalada verbal	
2. Fundamentos básicos para el análisis policial de dispositivos electrónicos	
3. La integración del bastón extensible en la policía local. Metodología, conocimiento y criterios	
4. Tecnologías aplicadas a la seguridad ciudadana: videocámaras, drones y vigilancia inteligente.	
5. La grabación de imágenes de la policía local en las intervenciones policiales	
 NOTICIAS	 PG.116
 DESCUENTOS	 PG.127

Artículos

COMUNICACIÓN POLICIAL Y DESESCALADA VERBAL



AUTOR: JUAN JOSÉ DELGADO IGLESIAS

COMUNICACIÓN POLICIAL Y DEESCALADA VERBAL

Autor: Juan José Delgado Iglesias

EPÍLOGO

La creciente complejidad de las intervenciones policiales en la sociedad actual, caracterizada por una mayor diversidad cultural, el incremento de situaciones de crisis de salud mental y unas expectativas ciudadanas cada vez más exigentes en cuanto al trato recibido, ha convertido la competencia comunicativa en una de las herramientas más valiosas de las que dispone el agente de Policía Local.

Durante años de servicio activo, la evidencia se acumula intervención a intervención: la diferencia entre una actuación que escala innecesariamente y otra que logra resolver la situación sin recurrir a la fuerza no siempre radica en la norma aplicada ni en la rapidez de la respuesta, sino en la calidad del contacto humano establecido en los primeros momentos. Esa observación, que en un principio puede parecer intuitiva, tiene hoy una base científica sólida y creciente que este trabajo ha intentado recoger y trasladar al lenguaje y a los problemas concretos del agente de proximidad.

La elaboración de esta publicación ha supuesto un esfuerzo de síntesis entre la psicología científica y la práctica policial cotidiana. Se ha procurado que cada concepto teórico encuentre su reflejo en situaciones reconocibles para cualquier agente que trabaje en la calle, con la convicción de que el conocimiento solo adquiere valor real cuando puede aplicarse en el momento y en el lugar en que se necesita.

La desescalada verbal no es una técnica blanda ni una concesión a la debilidad institucional: es, en muchos casos, la forma más eficaz y más segura de resolver una situación difícil, la que minimiza el riesgo para el agente, para el ciudadano y para la propia institución. Un agente que sabe comunicar no es menos firme que quien recurre de forma prematura a la autoridad coercitiva; es más completo, más versátil y, a largo plazo, más resiliente ante las demandas de una función pública que se ejerce con demasiada frecuencia en condiciones de alta exigencia emocional y escaso reconocimiento.

La Policía Local ocupa un lugar singular en el tejido social de los municipios: es la institución más cercana al ciudadano, la que acude en los momentos más vulnerables, la que gestiona conflictos que ningún otro servicio está dispuesto o en condiciones de asumir. Esa proximidad impone una responsabilidad comunicativa que no puede dejarse al azar ni resolverse únicamente con el instinto desarrollado en el servicio. Exige formación específica, reflexión permanente y acceso a los conocimientos que la investigación científica ha generado en este campo, trasladados al lenguaje y a los problemas reales del agente de a pie.

El reto pendiente para los cuerpos de Policía Local es que la formación en comunicación deje de ser un módulo aislado y voluntario para convertirse en un eje transversal de la formación inicial y del perfeccionamiento continuo. No porque lo exija una norma, sino porque los datos son inequívocos: los agentes mejor formados en habilidades

comunicativas intervienen con mayor eficacia, sufren menos desgaste emocional y generan una percepción ciudadana de la institución notablemente más positiva. Invertir en esta formación no es un gasto accesorio: es la política de seguridad más rentable que puede adoptar cualquier administración local.

La presente publicación «COMUNICACIÓN POLICIAL Y DESESCALADA VERBAL» se ha elaborado y publicado en colaboración con el Sindicato Independiente de Policía de Andalucía SIP-AN, para ser difundida en la Revista SIP-AN y en su versión de Publicación Electrónica, publicada en el Área de Formación — Biblioteca Virtual — Publicaciones de Interés Policial de www.sip-an.es, del citado sindicato.

ÍNDICE

ÍNDICE	
RESUMEN	
INTRODUCCIÓN	
DESARROLLO	
1. Neuropsicología del conflicto: lo que ocurre en el cerebro del ciudadano	
2. La ventana de tolerancia y el continuum de la escalada	
3. Escucha activa profunda y entrevista motivacional	
4. Comunicación no verbal avanzada: microexpresiones, proxemia y regulación	
5. Técnicas específicas de desescalada verbal	
6. La escalera conductual del cambio en situaciones de crisis	
7. Justicia procedimental y legitimidad policial	
8. El agente como variable psicológica: estrés, autorregulación y competencia emocional	
9. Protocolos de actuación comunicativa según perfil	
Persona en crisis emocional aguda	
Persona con trastorno mental en fase activa	
Persona bajo efectos de alcohol u otras sustancias	
Persona en riesgo de suicidio	
Víctima de violencia doméstica o de género	
10. Formación experiencial y práctica deliberada en comunicación policial	
CONCLUSIONES	
BIBLIOGRAFÍA	

RESUMEN

La comunicación constituye uno de los instrumentos más potentes y, al mismo tiempo, más subestimados del ejercicio de la función policial. En las intervenciones cotidianas de la Policía Local ante situaciones de conflicto, crisis o alteración del orden, la calidad de la interacción verbal y no verbal entre el agente y el ciudadano determina con frecuencia el desenlace de la situación con mayor fuerza que cualquier factor técnico o jurídico. El presente trabajo analiza, desde una perspectiva de psicología aplicada, los mecanismos neurobiológicos que subyacen al comportamiento humano en situaciones de conflicto, los modelos teóricos validados por la investigación científica y las técnicas prácticas de desescalada verbal. Se profundiza especialmente en conceptos como la ventana de tolerancia, la teoría polivagal, la entrevista motivacional y el modelo de la escalera conductual del cambio, trasladando su aplicación práctica al trabajo del agente de proximidad. Se analiza asimismo el impacto del estrés agudo y crónico en la calidad comunicativa del propio agente y se proponen estrategias de autorregulación emocional como componente indispensable de la competencia comunicativa policial. Se abordan también los fundamentos de la justicia procedimental y su relación directa con la percepción ciudadana de la legitimidad policial. El objetivo final es ofrecer un marco conceptual riguroso y herramientas prácticas contrastadas que contribuyan a mejorar la eficacia de las intervenciones, a reducir el recurso innecesario a la fuerza y a fortalecer la relación entre la Policía Local y la comunidad a la que sirve.

Palabras clave: desescalada verbal, comunicación policial, ventana de tolerancia, escucha activa, justicia procedimental, psicología del conflicto, Policía Local.

INTRODUCCIÓN

La Policía Local es, entre todas las instituciones del Estado, la que mantiene el contacto más directo, más frecuente y más cotidiano con la ciudadanía. Esta proximidad constituye al mismo tiempo su mayor fortaleza y su mayor desafío. El agente de proximidad no solo aplica la ley: gestiona relaciones humanas en condiciones frecuentemente adversas, negocia entre intereses en conflicto, acompaña a personas en los peores momentos de su vida y representa, para mucha gente, la única cara visible del Estado en situaciones de emergencia personal o familiar. Pocos roles profesionales exigen una competencia comunicativa tan amplia, tan intensa y desarrollada en condiciones tan desfavorables.

La pregunta sobre qué hace que una intervención policial sea eficaz va mucho más allá de los aspectos jurídicos y técnicos. La investigación en psicología policial acumulada en las últimas cuatro décadas apunta de manera consistente a que uno de los factores que más determina el resultado de una intervención es la calidad de la comunicación establecida entre el agente y el ciudadano. No el conocimiento normativo del agente, no su capacidad física, ni siquiera la gravedad objetiva de la situación: la calidad del contacto

humano que se establece en los primeros momentos. Este hallazgo, que puede parecer contraintuitivo desde determinadas culturas institucionales que siguen valorando la firmeza visible y la autoridad sin matices como marcadores centrales de la competencia profesional, tiene una base empírica sólida y creciente.

Los estudios realizados por Tom Tyler y sus colaboradores sobre justicia procedimental han demostrado que la percepción ciudadana de la legitimidad policial y la predisposición a cooperar con la policía dependen en mayor medida del trato recibido que del resultado concreto de la intervención. Las personas aceptan mejor un resultado desfavorable si sienten que han sido escuchadas y tratadas con respeto que un resultado favorable si sienten que han sido ignoradas o humilladas. Esta conclusión tiene implicaciones enormes y todavía insuficientemente asimiladas en la formación y en la cultura organizacional de la Policía Local española.

En este trabajo se analizan los mecanismos psicológicos que explican por qué determinadas formas de comunicación generan escalada y otras la reducen, y se describen las técnicas que la investigación y la práctica avalan como más eficaces. Se escribe desde la convicción de que un agente de Policía Local que comprende la psicología de las personas con quienes interactúa es, en todos los sentidos que importan en el ejercicio real del servicio público, un agente notablemente mejor y más seguro.

DESARROLLO

1. Neuropsicología del conflicto: lo que ocurre en el cerebro del ciudadano

Cuando un ciudadano entra en una situación de conflicto o se percibe amenazado por la presencia policial, en su cerebro se produce una cascada neurobiológica que tiene consecuencias directas y predecibles sobre su capacidad de comunicación, su toma de decisiones y su comportamiento. Comprender estos mecanismos no es un lujo académico: es una herramienta operativa de primera magnitud para el agente que quiere intervenir con eficacia.

El modelo de las tres capas del cerebro, propuesto por Paul MacLean (1990) y desarrollado posteriormente por Daniel Siegel, permite entender de forma práctica lo que ocurre en estas situaciones. El ser humano dispone de un sistema nervioso que, en términos evolutivos, ha priorizado la supervivencia sobre el razonamiento. La amígdala cerebral, estructura clave del sistema límbico, actúa como un sistema de alarma permanente que escanea el entorno en busca de señales de peligro y que puede desencadenar una respuesta de emergencia en milisegundos, antes de que la corteza prefrontal, responsable del pensamiento lógico y del control de impulsos, haya tenido tiempo de evaluar la situación. Daniel Goleman (1995) denominó a este fenómeno el “secuestro amigdalar”: la amígdala literalmente toma el control del comportamiento bloqueando el acceso a la corteza racional.

El secuestro amigdalar tiene consecuencias comunicativas específicas y predecibles. La persona que lo sufre experimenta una reducción significativa de su capacidad para

escuchar, para procesar argumentos complejos, para inhibir impulsos agresivos y para evaluar consecuencias futuras. Desde un punto de vista práctico, esto significa que intentar razonar con alguien en pleno pico de activación emocional es una estrategia con muy bajas probabilidades de éxito: la información verbal simplemente no llega con la misma eficacia. El primer objetivo del agente no debe ser convencer ni informar, sino reducir la activación emocional hasta un nivel que permita el diálogo productivo.

La teoría polivagal del neurocientífico Stephen Porges (2011) proporciona un marco aún más refinado para comprender la respuesta del sistema nervioso ante las situaciones de conflicto. Porges describió tres circuitos neurológicos jerárquicos que se activan en función del nivel de amenaza percibido. El primer circuito, el de mayor evolución filogenética, es el del sistema de participación social: cuando el entorno se percibe como seguro, este circuito permite la comunicación fluida, la empatía, el juego y la colaboración. El segundo circuito, evolutivamente más antiguo, es el simpático activado: genera la respuesta de lucha o huida y se activa cuando la amenaza supera el umbral de lo gestionable mediante el diálogo. El tercer circuito, el más primitivo y el que más puede alarmar a un agente no formado, es el parasimpático dorsal: genera la respuesta de congelación o colapso (freeze o shutdown), caracterizada por inmovilidad, disociación y apariencia de indiferencia o estupor.

La implicación práctica de la teoría polivagal es fundamental: el sistema nervioso del ciudadano responde antes al estado del agente que a sus palabras. El concepto de “neurocepción”, también acuñado por Porges, describe la capacidad inconsciente del sistema nervioso para detectar señales de seguridad o peligro en el entorno, incluyendo las que emite el sistema nervioso del interlocutor. Un agente con elevada activación simpática (acelerado, tenso, con tono de voz elevado) activará el sistema de alarma del ciudadano aunque sus palabras sean perfectamente correctas. Por el contrario, un agente que mantiene una activación controlada, un tono de voz tranquilo y una postura abierta, transmite señales de seguridad que favorecen la activación del circuito de participación social del ciudadano, facilitando el diálogo. En otras palabras: la regulación del estado interno del agente es la primera y más eficaz técnica de desescalada.

La hipótesis de la humillación, desarrollada por investigadores como James Gilligan (1997) a partir de su trabajo clínico con reclusos condenados por violencia extrema, apunta a que el detonante más común de la agresión grave en los seres humanos no es el dolor físico ni el miedo, sino la percepción de haber sido profundamente humillados o menospreciados. Gilligan concluyó, tras décadas de entrevistas, que detrás de la mayoría de los actos de violencia grave se encontraba la misma experiencia subjetiva: la persona sentía que había sido tratada como si no valiese nada, como si no fuera digna de respeto. La implicación para la comunicación policial es directa: un ciudadano que siente que el agente le falta al respeto, que le menosprecia o que le trata como un problema y no como una persona, es un ciudadano cuyo riesgo de escalada aumenta de forma significativa. La cortesía y el respeto no son concesiones al ciudadano: son herramientas de gestión del riesgo.

La teoría de la atribución de Weiner (1986) aporta otro mecanismo psicológico relevante.

Las personas en estado de activación emocional tienden a realizar atribuciones causales rápidas y frecuentemente incorrectas sobre el comportamiento de los demás. Un ciudadano que percibe la intervención policial como injustificada o arbitraria atribuirá la actuación del agente a motivos hostiles o discriminatorios, lo que intensificará su reacción defensiva. El agente que explica brevemente el motivo de su intervención (“me han avisado de que ha habido una discusión y me necesitan aquí”) reduce la posibilidad de que el ciudadano realice atribuciones negativas y facilita una respuesta más cooperativa.

2. La ventana de tolerancia y el continuum de la escalada

El psicólogo Dan Siegel (1999) desarrolló el concepto de “ventana de tolerancia” para describir la zona óptima de activación del sistema nervioso en la que el ser humano puede funcionar con eficacia: pensar con claridad, sentir de forma proporcionada y relacionarse de manera constructiva. Dentro de esta ventana, el individuo tiene acceso pleno a sus recursos cognitivos, emocionales y sociales. Fuera de ella, el funcionamiento se deteriora de manera predecible.

La ventana de tolerancia tiene dos bordes. El borde superior corresponde a la hiperactivación o hiperexcitación: la persona se encuentra en modo de lucha o huida, con el sistema simpático dominante. Los signos observables incluyen agitación motora, habla rápida y desorganizada, rostro enrojecido, incapacidad para escuchar, pensamiento dicotómico (todo o nada) y respuestas emocionales desproporcionadas. Es la zona en la que se encuentra la mayoría de los ciudadanos en conflicto activo que el agente de Policía Local debe gestionar. El borde inferior corresponde a la hipoactivación: el sistema nervioso ha superado el umbral de lo gestionable y se ha producido una desconexión protectora. Los signos incluyen mirada pérdida, voz apagada, movimientos lentos, incapacidad para responder preguntas simples, aparente indiferencia o ausencia de reacción. Esta es la zona en la que se encuentran frecuentemente las víctimas de violencia doméstica cuando la policía acude, o las personas que han sufrido una experiencia traumática reciente.

Para el agente, aprender a identificar rápida y correctamente en cuál de las dos zonas se encuentra el ciudadano es fundamental, porque las técnicas de intervención son radicalmente diferentes. Ante la hiperactivación, el objetivo es contener y calmar: reducir estímulos, bajar el propio tono de voz, ofrecer espacio físico, validar la emoción, evitar la confrontación directa. Ante la hipoactivación, el objetivo es activar de forma gradual y respetuosa: el contacto visual sostenido, la voz con mayor energía, el ofrecimiento de agua o de contacto físico (con los límites legales y culturales que corresponda), preguntas simples y directas que requieran respuesta. Confundir ambos estados o aplicar las mismas técnicas a los dos puede ser contraproducente o incluso peligroso.

La investigación sobre el estrés traumático ha demostrado que la anchura de la ventana de tolerancia no es igual para todas las personas: factores como la historia de trauma previo, los estilos de apego, el consumo de sustancias y las condiciones de vida pueden

estrecharla significativamente. Una persona con una historia de trauma complejo puede pasar de un estado aparentemente tranquilo a una desregulación completa ante un estímulo que a un observador externo puede parecer insignificante (un gesto brusco, un tono de voz elevado, una proximidad inesperada). Este fenómeno, conocido como disparo traumático o trauma trigger, explica muchas de las reacciones que los agentes describen como “incomprensibles” o “desproporcionadas” en sus intervenciones.

Patricia Ogden, una de las principales desarrolladoras de la psicoterapia sensoriomotriz, ha señalado que el cuerpo recuerda el trauma antes de que la mente consciente lo reconozca. Las posturas corporales del agente, el tono de su voz, la distancia física o incluso el uniforme pueden activar recuerdos somáticos de experiencias traumáticas previas en el ciudadano, generando reacciones que no están relacionadas con la situación presente sino con el pasado de esa persona. El agente que comprende esto puede interpretar esas reacciones de forma más precisa y responder con mayor eficacia.

El continuum de la escalada describe el proceso mediante el cual una situación de baja conflictividad puede evolucionar hacia la violencia a través de una serie de etapas reconocibles. En cada etapa, hay una ventana de oportunidad para la intervención comunicativa que se va estrechando progresivamente. Los investigadores en comportamiento hostil y gestión de conflictos han identificado que la mayoría de los incidentes violentos en espacios públicos no son actos impulsivos sin precursores: existe una progresión que incluye conductas de advertencia verbales y no verbales que el agente entrenado puede detectar y ante las que puede intervenir preventivamente. La formación en reconocimiento de estas señales de escalada es, paradójicamente, una de las áreas más descuidadas en los planes formativos de la Policía Local española.

3. Escucha activa profunda y entrevista motivacional

La escucha activa es, en el contexto de la psicología clínica y la comunicación terapéutica, un proceso deliberado y estructurado que va mucho más allá de la simple ausencia de interrupciones. Su desarrollo conceptual se debe fundamentalmente a Carl Rogers (1957), quién la definió como uno de los ingredientes esenciales de la relación terapéutica eficaz, y fue sintetizada posteriormente con fines aplicados en el modelo de la Entrevista Motivacional desarrollado por William Miller y Stephen Rollnick (1991), cuya utilidad en contextos policial ha sido ampliamente documentada.

La técnica OARS, acrónimo de la Entrevista Motivacional, resume las cuatro habilidades básicas de la escucha activa profunda. La O corresponde a las preguntas abiertas (Open questions): son las que no pueden responderse con un simple sí o no y que invitan a la persona a elaborar su experiencia. “Cuénteme que ha pasado” o “cómo se siente usted en este momento” son preguntas abiertas que transmiten disponibilidad y generan más información útil que cualquier batería de preguntas cerradas. La A corresponde a las afirmaciones (Affirmations): son reconocimientos genuinos de las fortalezas o esfuerzos de la persona, no halagos superficiales. Hay que reconocer que una persona ha hecho algo bien o que está haciendo un esfuerzo por cooperar tiene un efecto directo sobre su disposición a continuar cooperando, a través del mecanismo de refuerzo positivo y de la

activación del sistema de recompensa cerebral. La R corresponde a la escucha reflexiva (Reflective listening): es el elemento más poderoso y difícil de dominar de la escucha activa. No se trata de repetir como un loro lo que ha dicho la persona (eco literal), sino de reflejar el significado profundo o la emoción que subyace a sus palabras. Si alguien dice “no me interesa lo que tengáis que decir”, la reflexión literal sería “no te importa lo que digo”; la reflexión profunda sería “estas muy cansado de sentir que nadie te escucha”. Hay una diferencia abismal entre ambas. La S corresponde a los resúmenes (Summaries): consisten en recopilar periódicamente lo que la persona ha comunicado, lo que tiene un triple efecto: demostrar que se ha prestado atención, organizar la información y dar a la persona la oportunidad de corregir posibles malentendidos.

La distinción que Miller y Rollnick establecen entre la empatía y la simpatía tiene especial relevancia en el contexto policial. La simpatía implica compartir el estado emocional del otro (“yo también me sentiría fatal en tu lugar”): tiene el efecto paradójico de centrar la atención en el agente y puede resultar poco creíble en un contexto policial. La empatía, en cambio, consiste en comprender la experiencia del otro desde su propio marco de referencia, sin necesariamente compartirla ni validar las acciones que de ella se derivan (“entiendo que esta situación te resulta muy injusta”). La empatía puede coexistir con la autoridad, con la discrepancia y con la firmeza: no implica ceder ni estar de acuerdo. Este es un matiz que muchos agentes no han integrado y que les lleva a evitar el lenguaje empático por temor a perder autoridad.

El investigador William Ickes (1997) acuñó el concepto de “exactitud empática” (empathic accuracy) para describir la capacidad de inferir correctamente los estados mentales (pensamientos, sentimientos, intenciones) del interlocutor a partir de sus conductas observables. La exactitud empática no es una habilidad mágica ni un talento innato: es una habilidad que puede entrenarse sistemáticamente mediante la observación atenta, el análisis de la comunicación y la retroalimentación. Los agentes con alta exactitud empática toman decisiones significativamente mejores en situaciones de conflicto porque disponen de una representación más precisa de lo que está ocurriendo en la mente del ciudadano.

Uno de los errores más comunes y dañinos en la práctica de la escucha activa por parte de agentes es lo que los psicólogos denominan “escucha evaluativa”: escuchar para juzgar, para buscar inconsistencias o para preparar la respuesta siguiente, en lugar de escuchar para comprender. La escucha evaluativa es detectable para la mayoría de las personas (aunque no puedan articular por que la detectan) y activa una respuesta defensiva que dificulta la comunicación genuina. Entrenarse para suspender el juicio temporalmente, incluso cuando la situación invita al juicio, es una de las habilidades más difíciles y valiosas que un agente puede desarrollar.

Los “mínimos alentadores” son pequeñas señales verbales y no verbales que el agente puede emitir de forma periódica para indicar que está siguiendo el relato de la persona: un leve asentimiento de cabeza, un “entiendo”, un “sigo”, un “cuénteme más”. Aunque parecen triviales, tienen un efecto documentado sobre la disposición de la persona a continuar comunicando, al activar el circuito de recompensa social del cerebro. Su

ausencia, por el contrario, puede ser interpretada como desinterés y generar inhibición comunicativa.

4. Comunicación no verbal avanzada: microexpresiones, proxemia y regulación

El lenguaje no verbal constituye el sustrato sobre el que descansa toda comunicación en situaciones de alta carga emocional. Esta afirmación no es una metáfora: tiene una base neurológica precisa. El sistema límbico, que procesa las emociones y genera las respuestas de emergencia, evalúa los estímulos no verbales del entorno de forma preconsciente, en una escala de tiempo de milisegundos, mucho antes de que la corteza prefrontal haya procesado el contenido verbal del mensaje. Esto significa que el impacto no verbal de la presencia del agente se ha producido ya antes de que haya pronunciado una sola palabra.

Paul Ekman y Wallace Friesen (1978) identificaron y catalogaron las microexpresiones faciales: gestos emocionales de alta intensidad y muy corta duración (entre 1/25 y 1/5 de segundo) que reflejan el estado emocional real de una persona antes de que esta pueda suprimirlos o enmascáralos con una expresión social apropiada. Las microexpresiones corresponden a las siete emociones básicas universales descritas por Ekman: alegría, tristeza, ira, miedo, asco, sorpresa y desprecio. En el contexto policial, la capacidad de detectar microexpresiones tiene valor tanto para evaluar la credibilidad y el estado emocional del interlocutor como para tomar decisiones tácticas más informadas. La microexpresión de desprecio (contracción unilateral del labio superior) es particularmente relevante porque es el predictor más fiable de hostilidad sostenida, incluso cuando la persona mantiene un discurso verbal aparentemente cooperativo.

Edward Hall (1966) definió la proxemia como el estudio de la dimensión espacial de la comunicación humana y estableció cuatro zonas de distancia interpersonal cuya utilización varía según la relación entre los interlocutores y el contexto cultural. La zona íntima (0-45 cm) está reservada para las relaciones de mayor confianza e intimidad. La zona personal (45-120 cm) es la empleada en conversaciones cotidianas entre personas conocidas. La zona social (120-360 cm) corresponde a las interacciones formales. La zona pública (más de 360 cm) es la de los discursos y las presentaciones. En situaciones de conflicto, la invasión de la zona íntima o personal de una persona sin su consentimiento activa automáticamente una respuesta de alarma en el sistema nervioso, con independencia de las intenciones del agente. La distancia óptima para iniciar una intervención de desescalada es la zona social, reduciéndola gradualmente y con señales de seguridad en la medida en que la situación lo permite.

La teoría de los sistemas de activación del sistema nervioso de Porges tiene implicaciones directas sobre cómo el agente debe usar su voz. El nervio vago ventral, que regula el sistema de participación social, está anatómicamente vinculado a los músculos que controlan la prosodia vocal (la melodía, el ritmo y la entonación del habla). Una voz con prosodia rica, que sube y baja de forma natural, transmite señales de seguridad que activan el sistema de participación social del interlocutor. Una voz plana, monótona o excesivamente rápida transmite señales de alarma que pueden activar el

sistema simpático. La velocidad del habla es particularmente importante: hablar a velocidad reducida da a la persona más tiempo para procesar lo que escucha y transmite calma, mientras que hablar rápido puede interpretarse como nerviosismo o urgencia y elevar la activación del interlocutor.

El fenómeno de la sincronía conductual o “isopraxis”, descrito en la literatura de comunicación no verbal, tiene una base neurocientífica: los sistemas de neuronas espejo identificados por Rizzolatti y sus colaboradores (1996) son estructuras neurales que se activan tanto cuando el individuo realiza una acción como cuando observa a otro realizarla. Estos sistemas son el sustrato neurológico de la imitación inconsciente y de la empatía somática. El agente que adopta deliberadamente una postura tranquila, una respiración pausada y una velocidad de habla reducida puede inducir, a través de este mecanismo, una sincronización gradual del estado físico del interlocutor hacia una menor activación. Esta técnica, conocida en la literatura anglosajona como “pacing and leading”, requiere práctica y autenticidad: si el agente la aplica de forma mecánica, sin que su propio estado interno sea genuinamente tranquilo, el resultado es incoherente y puede ser detectado como manipulación.

El contacto físico merece una mención específica por su complejidad en el contexto policial. La háptica (el estudio del tacto en la comunicación humana) ha documentado que el contacto físico apropiado puede tener efectos potentemente calmantes: reduce el cortisol, activa la oxitocina y señala de forma directa la seguridad del entorno. Sin embargo, en el contexto policial, el contacto físico no solicitado sobre una persona en estado de activación emocional elevada puede ser percibido como amenazante o invasivo y desencadenar una respuesta defensiva intensa. En personas con historia de trauma físico, el contacto no anunciado puede provocar reacciones de pánico o disociación. La regla práctica es clara: antes de establecer cualquier contacto físico en una intervención de desescalada (por ejemplo, una mano sobre el hombro para tranquilizar), el agente debe asegurarse de que existe al menos un nivel mínimo de rapport establecido y de que el contexto cultural y personal de la persona lo hace apropiado.

5. Técnicas específicas de desescalada verbal

El conocimiento de los mecanismos psicológicos descritos en los apartados anteriores tiene valor práctico solo si se traduce en técnicas concretas y entrenadas que el agente pueda aplicar en condiciones de estrés. A continuación, se describen las técnicas de desescalada verbal mejor documentadas en la literatura científica y en la práctica policial, con especial atención a los mecanismos que explican su eficacia y a las condiciones en que son más aplicables.

El etiquetado emocional, sistematizado por el negociador del FBI Chris Voss en su obra “Never Split the Difference” (2016), consiste en identificar y nombrar de forma tentativa la emoción que el agente percibe en el interlocutor, formulada como una observación y no como una afirmación definitiva: “Parece que esto te tiene muy agotado”, “Da la sensación de que estas muy asustado”, “Parece que te sientes muy injustamente

tratado”. La formulación tentativa es deliberada: permite a la persona corregirla si no es precisa, lo que en sí mismo genera comunicación. El etiquetado emocional tiene un efecto neurobiológico documentado: nombrar una emoción reduce la activación de la amígdala cerebral, un fenómeno denominado “afecto como información” que Lieberman y colaboradores (2007) demostraron mediante técnicas de neuroimagen. En términos coloquiales, poner palabras a una emoción intensa la hace más manejable para quién la experimenta.

El espejejo verbal (mirroring), también descrito por Voss, consiste en repetir, en tono de pregunta, las últimas dos o tres palabras que ha dicho la persona. Si alguien dice “es que ya no puedo más con esta situación”, el agente responde “ya no puedes más”. La simplicidad de la técnica contrasta con su eficacia: invita a la persona a continuar elaborando su discurso (lo que reduce la activación emocional), demuestra que el agente está escuchando y no introduce ningún elemento evaluativo que pueda activar defensividad. El espejejo verbal es especialmente útil en los primeros momentos de una intervención, cuando el nivel de desconfianza es mayor y cuando es más difícil hacer afirmaciones o reflexiones complejas sin que sean rechazadas.

La técnica del acuerdo parcial permite reconocer los elementos de legitimidad que contiene la queja del ciudadano sin abandonar la posición de autoridad ni validar la totalidad del comportamiento. Ante la afirmación “siempre venís a molestar a los vecinos honrados y dejáis tranquilos a los que hacen ruido”, el agente puede responder: “Es verdad que el ruido en esta calle es un problema real y que lleva tiempo sin resolverse. Cuénteme exactamente qué ha pasado esta noche”. Esta respuesta cumple varias funciones simultáneas: válida la queja parcial, demuestra que el agente ha escuchado, dirige la conversación hacia la situación presente y no refuerza ni rechaza la generalización hostil. El acuerdo parcial requiere autenticidad: el agente debe encontrar un elemento genuinamente válido en la queja y no fabricarlo, porque la falsedad en este contexto es fácilmente detectable y contraproducente.

La sustitución de “pero” por “y” es una técnica aparentemente menor, pero con efectos comunicativos significativos. Cuando se conecta una validación con una corrección mediante la conjunción “pero”, el “pero” funciona como un borrador semántico que anula todo lo que viene antes: “entiendo que estas enfadado, PERO tienes que calmarte” transmite principalmente “tienes que calmarte”. Cuando se usa “y”, las dos ideas coexisten sin que ninguna borre a la otra: “entiendo que estas enfadado, Y al mismo tiempo necesito que bajemos el tono para poder resolverlo”. La diferencia puede parecer sutil, pero en el proceso de escucha del interlocutor produce un efecto cualitativamente distinto.

Las preguntas orientadas a soluciones, derivadas de la terapia breve centrada en soluciones (De Shazer, 1985), resultan especialmente útiles cuando la persona lleva tiempo hablando del problema sin que se vislumbre una salida. “Si mañana, al despertar, esta situación estuviera de alguna manera mejor, ¿qué sería lo primero que notarías?” o “En algún momento en el pasado, ¿hubo algo que os ayudó a gestionar esto de una forma que os funcionará?” desplazan el foco del problema al recurso, activan la memoria

de momentos de competencia y generan una orientación psicológica hacia el futuro que contrasta benéficamente con el estado de impotencia que suele acompañar a los conflictos crónicos.

El ofrecimiento de opciones limitadas, bien conocido en la literatura de negociación, merece una explicación psicológica más profunda de la que habitualmente se le da. La percepción de tener cierta agencia, de poder elegir entre alternativas, aunque estas sean limitadas, activa circuitos cerebrales relacionados con el control y la predicción que se ven bloqueados por la coerción directa. La impotencia aprendida, descrita por Martin Seligman, es un estado en el que el individuo ha llegado a la conclusión de que sus acciones no tienen ningún efecto sobre su entorno: en ese estado, la resistencia pasiva o la agresión se convierten en los únicos comportamientos que quedan disponibles. El ofrecimiento de opciones, incluso muy limitadas, rompe ese estado al restablecer la percepción de agencia.

6. La escalera conductual del cambio en situaciones de crisis

El Modelo de la Escalera Conductual del Cambio (Behavioral Change Stairway Model, BCSM) fue desarrollado por la División de Respuesta a Incidentes Críticos del FBI y es actualmente uno de los marcos más utilizados en la formación de negociadores de crisis a nivel mundial. Su estructura en cinco escalones describe el proceso por el que una persona en estado de crisis puede pasar de la resistencia activa a la colaboración voluntaria, y subraya un principio metodológico que tiene implicaciones profundas para cualquier intervención policial: no se pueden saltarse escalones.

El primer escalón es la escucha activa. No puede producirse nada productivo si la persona no percibe que está siendo genuinamente escuchada. La escucha activa no es aquí un prelude educado antes de pasar al tema importante: es el tema importante. Los negociadores de crisis del FBI invierten una proporción muy elevada de su tiempo total en este primer escalón porque saben que es el único camino hacia los siguientes. Los intentos de llegar directamente a la negociación o a la persuasión sin haber establecido primero la escucha activa fracasan de forma sistemática.

El segundo escalón es la empatía. Solo cuando la persona siente que sus palabras han sido genuinamente escuchadas puede comenzar a surgir una conexión emocional. La empatía en este contexto no es un estado de fusión emocional con el interlocutor: es la demostración activa de que el agente comprende la experiencia de la persona desde su propio marco de referencia. Los negociadores del FBI utilizan la frase “parece que...” de forma consistente para formular reflexiones empáticas que no implican acuerdo, pero sí comprensión.

El tercer escalón es el rapport. El rapport no se decide ni se declara: se construye gradualmente a través de la acumulación de intercambios en los que la escucha activa y la empatía han sido consistentes. Una persona que ha experimentado que el agente la escucha de verdad y comprende su experiencia puede empezar a sentir que existe una relación de suficiente confianza para continuar comunicando. El rapport en una intervención de crisis no requiere simpatía personal ni acuerdo de valores: requiere

consistencia, respeto y autenticidad.

El cuarto escalón es la influencia. Solo cuando existe rapport puede el agente comenzar a introducir perspectivas alternativas, a sugerir soluciones o a pedir cambios de comportamiento con alguna probabilidad de que sean escuchados y considerados. Cualquier intento de influir antes de haber establecido rapport encontrará resistencia o será ignorado. Este es uno de los errores más frecuentes en las intervenciones policial es ordinarias: los agentes intentan convencer o instruir antes de haber establecido el nivel mínimo de conexión emocional que hace la persuasión posible.

El quinto escalón es el cambio conductual. Es el resultado natural de haber recorrido los cuatro escalones anteriores con consistencia: la persona modifica su comportamiento de forma voluntaria porque ha encontrado en la interacción con el agente una razón para hacerlo. El cambio conductual obtenido mediante la presión o la coerción directa es frecuentemente superficial y efímero. El obtenido mediante el proceso de la escalera conductual tiende a ser más estable y menos propenso a la recaída o a la resistencia pasiva posterior.

La principal implicación práctica del BCSM para los agentes de Policía Local es de orden metodológico: cuando una intervención no progresa, la causa más frecuente es que se han intentado quemar escalones. El agente que siente que la persona no le escucha, que no responde a la razón o que se resiste a cualquier propuesta, debe preguntarse en que escalón se encuentra realmente la intervención y volver al anterior si es necesario. En la mayoría de los casos, volver a la escucha activa y la empatía cuando la situación se ha estancado es la decisión táctica más eficaz disponible.

7. Justicia procedimental y legitimidad policial

El catedrático de derecho y psicología Tom Tyler (1990, 2006) ha consagrado décadas de investigación empírica a una pregunta aparentemente sencilla: ¿por qué las personas obedecen la ley? Sus conclusiones, reproducidas de forma consistente en múltiples países y contextos, son contraintuitivas desde la perspectiva del modelo disuasorio clásico. Las personas no obedecen la ley principalmente por miedo a las consecuencias: obedecen, o no, principalmente en función de si perciben que las instituciones que la aplican son legítimas. Y la percepción de legitimidad depende de forma predominante de la percepción de justicia procedimental: del trato que reciben en las interacciones con los agentes institucionales.

Tyler identificó cuatro componentes de la justicia procedimental que los ciudadanos valoran de forma consistente. El primero es la voz: la percepción de haber tenido la oportunidad de expresar su punto de vista antes de que se tomase una decisión que les afectaba, con independencia de si esa expresión tuvo influencia en la decisión final. El segundo es la neutralidad: la percepción de que el agente ha actuado de forma imparcial, basándose en hechos y normas y no en prejuicios personales. El tercero es el respeto: la percepción de haber sido tratado con dignidad durante toda la interacción. El cuarto es la confianza en los motivos: la percepción de que el agente actúa por razones genuinamente orientadas al bien común y no por interés propio, por hostigamiento o

por capricho.

El hallazgo más relevante de Tyler desde el punto de vista práctico es el siguiente: las personas aceptan mejor un resultado desfavorable (una multa, una detención, un orden de desalojo) si sienten que el proceso mediante el que se ha llegado a ese resultado ha sido justo, que un resultado favorable obtenido mediante un proceso percibido como injusto. En otras palabras: el proceso importa tanto o más que el resultado. Un ciudadano al que se le pone una multa pero que siente que ha sido escuchado y tratado con respeto es menos probable que desarrolle resentimiento hacia la institución policial que un ciudadano al que se le anula la multa pero que siente que ha sido tratado con arrogancia o indiferencia.

Las implicaciones de esta investigación para el lenguaje específico que usa el agente son directas. El uso del nombre de la persona (“señor García”) en lugar de un tratamiento impersonal, la explicación breve del motivo de la intervención antes de pedir identificación, el ofrecimiento de la oportunidad de explicar la versión del ciudadano antes de tomar una decisión, el agradecimiento explícito por la cooperación recibida, la despedida respetuosa al final de la intervención: todos estos elementos son pequeños actos comunicativos que contribuyen a la percepción de justicia procedimental y que, acumulados a lo largo de miles de interacciones, determinan la percepción social de la legitimidad de la Policía Local en la comunidad.

El lenguaje que el agente utiliza para formular sus peticiones o instrucciones tiene también implicaciones sobre la percepción de legitimidad. Las instrucciones en imperativo sin justificación (“parece ahí”, “deme el carnet”, “abra el maletero”) pueden ser legalmente correctas, pero comunicativamente costosas: activan la reactancia psicológica (Brehm, 1966) y refuerzan la percepción de arbitrariedad. Las mismas instrucciones formuladas con una breve justificación (“necesito que se pare ahí para poder hablar con seguridad para los dos”, “necesito ver su documentación para identificarle correctamente”) producen tasas de cumplimiento significativamente más altas y menor percepción de coerción, sin que el agente ceda en su autoridad ni en sus obligaciones legales.

La investigación de Tyler tiene también implicaciones importantes para el largo plazo. Las comunidades que perciben que la policía que trabaja en su territorio actúa con justicia procedimental son más propensas a colaborar con las investigaciones, a denunciar delitos, a proporcionar información sobre actividades sospechosas y a intervenir como testigos. En otras palabras: la justicia procedimental en el plano individual acumula capital social institucional que tiene efectos directos sobre la eficacia policial en términos de seguridad pública. La comunicación respetuosa no es solo una cuestión ética: es una herramienta estratégica de eficacia policial a largo plazo.

8. El agente como variable psicológica: estrés, autorregulación y competencia emocional

Una de las paradojas fundamentales de la comunicación policial en situaciones de conflicto es que el agente debe comunicarse con mayor eficacia precisamente en los

momentos en que su propio sistema nervioso esta más activado. El estrés del servicio policial no es una variable ajena a la comunicación: es una variable que la condiciona de forma directa y sistemática, y cualquier análisis de la comunicación policial que no tenga en cuenta el estado psicológico del propio agente está incompleto.

Es importante distinguir entre tres conceptos que frecuentemente se confunden en la literatura sobre bienestar policial. El síndrome de desgaste profesional o burnout, descrito por Maslach y Jackson (1981), se caracteriza por el agotamiento emocional (sentir que los recursos emocionales se han agotado), la despersonalización (adoptar una actitud distante o indiferente, incluso cínica, hacia las personas con quienes se trabaja) y la reducción de la realización personal (sentir que el trabajo ya no tiene sentido o valor). El estrés traumático secundario o fatiga por compasión, descrito por Figley (1995), es un proceso diferente: surge de la exposición acumulada al sufrimiento ajeno y produce síntomas similares al estrés postraumático (intrusiones, evitación, hipervigilancia). El estrés agudo operacional, en cambio, es una respuesta adaptativa y normal del sistema nervioso ante situaciones de alta demanda: es funcional en dosis adecuadas, pero deteriora el rendimiento cuando supera el nivel óptimo.

El efecto específico del estrés agudo sobre la comunicación incluye fenómenos bien documentados en la literatura de psicología policial. La visión de túnel perceptivo reduce la atención a los estímulos periféricos y hace al agente menos sensible a las señales no verbales del entorno, precisamente las que más información aportan sobre el estado emocional del interlocutor. La exclusión auditiva o tunnel hearing produce una reducción transitoria de la capacidad de procesar información verbal compleja. El pensamiento dicotómico se intensifica, dificultando la generación de opciones a la solución más obvia. La tolerancia a la ambigüedad disminuye, lo que puede llevar a conclusiones precipitadas. Todos estos efectos se combinan para producir exactamente el tipo de comunicación que menos conviene en situaciones de alta tensión: rápida, rígida, evaluativa y poco sensible al estado del interlocutor.

La autorregulación emocional, que Gross y Thompson (2007) definen como el conjunto de procesos mediante los cuales los individuos influyen sobre las emociones que tienen, cuando las tienen y como las experimentan y expresan, es una competencia central del agente de policía que trabaja en situaciones de alta demanda emocional. Daniel Goleman (1995) identificó la autorregulación como uno de los cuatro pilares de la inteligencia emocional, junto con la autoconciencia, la motivación y las habilidades sociales, y señaló que la autorregulación eficaz requiere primero autoconciencia: no es posible regular un estado emocional que no se reconoce.

Las técnicas de autorregulación con mejor soporte empírico para profesionales de alta demanda incluyen la respiración diafragmática controlada, que activa el sistema nervioso parasimpático a través del nervio vago y puede reducir la frecuencia cardíaca en cuestión de dos a tres minutos. La práctica de mindfulness o atención plena, avalada por más de un centenar de estudios controlados en poblaciones de alta demanda, mejora la regulación emocional, reduce el impacto del estrés agudo y mejora la precisión perceptiva en situaciones de tensión. El ensayo mental previo a intervenciones de alto

riesgo, conocido en psicología del deporte como visualización o rehearsal mental, ha demostrado reducir la respuesta de estrés y mejorar el rendimiento bajo presión.

La cultura institucional policial desempeña un papel crucial en la autorización o negación de estas estrategias de autorregulación. En contextos donde expresar vulnerabilidad emocional se percibe como debilidad profesional, los agentes que experimentan dificultades tienden a suprimir sus estados emocionales en lugar de gestionarlos. La supresión emocional, a diferencia de la regulación, no reduce la activación fisiológica: la mantiene o la aumenta, al tiempo que consume recursos cognitivos adicionales. El resultado es un agente que parece calmado externamente pero que está internamente más activado que si hubiera expresado lo que siente, y cuya capacidad cognitiva y comunicativa está reducida por el esfuerzo de supresión. Las instituciones que promueven el bienestar psicológico de sus agentes, lejos de debilitarlos, están invirtiendo en su eficacia operativa.

9. Protocolos de actuación comunicativa según perfil

La Policía Local interactúa diariamente con una variedad de perfiles psicológicos cuyas necesidades comunicativas son radicalmente distintas. La aplicación de un protocolo comunicativo uniforme a todos los perfiles es un error que multiplica el riesgo de escalada y reduce la eficacia de la intervención. Lo que se describe a continuación no son estereotipos diagnósticos, sino guías prácticas para adaptar la comunicación a las características del estado psicológico del interlocutor en el momento de la intervención.

Persona en crisis emocional aguda

El signo distintivo de la crisis emocional aguda es la desregulación del sistema nervioso: la persona se encuentra claramente por encima del borde superior de su ventana de tolerancia. Motricidad agitada, discurso rápido o fragmentado, llanto intenso, gritos, incapacidad para escuchar preguntas simples son señales reconocibles. En este estado, el cerebro no puede procesar información compleja. El objetivo comunicativo del agente no es resolver el conflicto ni obtener información: es regular el sistema nervioso de la persona hasta llevarlo dentro de su ventana de tolerancia. Las herramientas en este caso son el tono de voz pausado y calmado (que actúa como una señal de seguridad para el sistema nervioso del interlocutor), la reducción de estímulos sensoriales cuando sea posible, el etiquetado emocional (“parece que estás muy asustada”), la validación sin evaluación (“tiene sentido que te sientas así”) y el mantenimiento de la presencia tranquila del agente como ancla de seguridad. Las peticiones de información deben posponerse hasta que la activación haya descendido a un nivel manejable.

Persona con trastorno mental en fase activa

La intervención con personas en fase activa de un trastorno mental (psicosis, episodio maníaco, crisis disociativa) requiere un conocimiento de base sobre el fenómeno clínico que no siempre está disponible en la formación policial estándar. En un episodio psicótico, la persona puede estar experimentando alucinaciones, delirios o pensamiento desorganizado que determinan su percepción de la realidad de forma completamente

diferente a la del agente. Intentar corregir las percepciones delirantes de forma directa (“eso no es verdad”, “nadie te está persiguiendo”) raramente funciona y frecuentemente intensifica la angustia y la desconfianza. La aproximación más eficaz consiste en conectar con la realidad emocional de la persona sin reforzar el contenido del delirio: “Parece que estas muy asustado. Eso debe ser muy difícil de vivir”. La coordinación rápida con los servicios de salud mental es imprescindible en la mayoría de estos casos, y el agente debe conocer los protocolos de coordinación interinstitucional de su municipio. El objetivo de la comunicación policial en estos casos no es resolver la situación clínica, sino mantener la seguridad y el vínculo hasta que intervengan los recursos especializados.

Persona bajo efectos de alcohol u otras sustancias

El consumo de alcohol y otras sustancias tiene efectos específicos sobre el sistema nervioso que el agente debe conocer para adaptar su comunicación. El alcohol en dosis altas produce desinhibición conductual (reducción de los umbrales de agresión y de vergüenza), pensamiento simplificado, discurso desorganizado y reducción de la capacidad de procesar argumentos complejos. Además, los estímulos emocionales tienen un peso desproporcionado sobre el comportamiento: un tono de voz que percibe como amenazante puede desencadenar una respuesta agresiva que en estado de sobriedad no se habría producido. Las reglas prácticas para este perfil incluyen: usar frases muy cortas y simples, mantener un tono de voz absolutamente neutro, evitar cualquier contacto físico no anunciado, no intentar razonar sobre consecuencias futuras (la intoxicación limita drásticamente la capacidad de proyección temporal), y ser extremadamente consciente del propio lenguaje no verbal, que la persona intoxicada puede leer de forma hipertrofiada.

Persona en riesgo de suicidio

La intervención comunicativa ante una persona que está considerando quitarse la vida es uno de los escenarios más exigentes que un agente de Policía Local puede encontrar. La investigación en prevención del suicidio ha identificado errores comunicativos frecuentes que aumentan el riesgo. El primero es minimizar: “no es para tanto”, “tienes mucho por lo que vivir” invalidan la experiencia de la persona y pueden incrementar el aislamiento. El segundo es argumentar o persuadir mediante razón: la persona en crisis suicida frecuentemente ha llegado a su estado a través de un largo proceso de pensamiento que le parece perfectamente coherente desde dentro. La persuasión lógica externa rara vez modifica ese estado. El tercer error es prometer soluciones que el agente no puede garantizar. La técnica con mejor soporte empírico es la escucha activa profunda orientada a explorar el dolor específico que subyace a la ideación suicida (“cuénteme que es lo que más le duele en este momento”), la validación de ese dolor sin validar la solución suicida como única salida (“entiendo que el dolor que estas sintiendo es real y que se siente insoportable”), y la conexión con cualquier factor de protección que la persona pueda identificar (personas cercanas, responsabilidades, cosas por las que todavía hay algo de esperanza). El objetivo no es resolver el problema de fondo, que probablemente requiere intervención especializada: es mantener la seguridad de la persona el tiempo suficiente para que los recursos clínicos puedan

intervenir.

Víctima de violencia doméstica o de género

Las víctimas de violencia doméstica crónica presentan frecuentemente un estado psicológico que incluye hipervigilancia (un estado de alerta permanente que puede manifestarse como agitación o como congelación), vergüenza intensa (que puede llevar a minimizar o retirar la denuncia), lealtad ambivalente hacia el agresor (especialmente cuando existen hijos en común o dependencia económica) y desconfianza hacia las instituciones basada en experiencias previas de no ser creídas o de no recibir protección eficaz. El agente que acude a un domicilio por una llamada de violencia doméstica debe ser consciente de que la actitud inicial de la víctima puede ser de silencio, de negación o incluso de defensa del agresor, y que estas conductas no son indicadores de que el riesgo no existe. La entrevista con la víctima debe realizarse siempre en un espacio de máxima privacidad, sin la presencia del presunto agresor, con un tono que transmita neutralidad y credibilidad absoluta, y con el tiempo suficiente para que la víctima pueda articular su experiencia a su propio ritmo.

10. Formación experiencial y práctica deliberada en comunicación policial

La investigación sobre la adquisición de habilidades complejas ha establecido con claridad que el simple conocimiento de las técnicas no es suficiente para desarrollar la competencia comunicativa en situaciones de alta presión. Anders Ericsson (1993), cuyo trabajo sobre la práctica deliberada ha transformado la psicología del rendimiento de élite, demostró que la diferencia entre expertos y novatos en campos que requieren habilidades complejas no reside principalmente en el talento innato sino en la calidad y la cantidad de práctica estructurada. La práctica deliberada se distingue de la práctica ordinaria en varios aspectos: es específicamente orientada a mejorar los puntos débiles del desempeño (no solo a repetir lo que ya se hace bien), incluye retroalimentación precisa e inmediata sobre el rendimiento, y se realiza en condiciones de máxima atención y esfuerzo cognitivo.

El modelo Dreyfus de adquisición de habilidades (Dreyfus y Dreyfus, 1986) describe cinco estadios de competencia que son aplicables a la comunicación policial: novato, principiante avanzado, competente, proficiente y experto. En el estadio de novato, el agente aplica las reglas aprendidas de forma rígida y sin sensibilidad al contexto. En el estadio experto, el comportamiento es fluido, intuitivo y contextualmente ajustado, y la persona ya no puede describir fácilmente las reglas que sigue porque las ha interiorizado hasta el punto de que son automáticas. La formación en comunicación policial debe tener en cuenta este continuum y adaptar sus metodologías al estadio de desarrollo del agente. Las formaciones que transmiten reglas a agentes que aún no han desarrollado la sensibilidad contextual necesaria para aplicarlas con criterio pueden producir comportamientos rígidos que son peores que la actuación espontánea.

El role-playing o juego de roles con actores entrenados es la metodología formativa con mayor soporte empírico para el desarrollo de habilidades comunicativas en situaciones de alta presión. La clave de su eficacia no es la complejidad del escenario sino la calidad

de la retroalimentación posterior: un análisis detallado, conducido por un formador con competencia clínica, de que técnicas se han aplicado, en qué momento, con que efecto observable y que alternativas existían. Sin esta retroalimentación de calidad, el role-playing puede consolidar patrones ineficaces en lugar de corregirlos.

La simulación mediante realidad virtual ha comenzado a introducirse en la formación policial de algunos países con resultados prometedores. Los sistemas de entrenamiento inmersivo permiten registrar y analizar con precisión milimétrica la postura corporal del agente, su tono de voz, sus movimientos y sus tiempos de respuesta, proporcionando una retroalimentación objetiva que un formador humano dificultosamente puede proporcionar con la misma precisión. Sin embargo, la realidad virtual tiene limitaciones que los fabricantes no siempre destacan suficientemente: los avatares digitales no producen exactamente las mismas respuestas emocionales en el agente que un interlocutor humano real, lo que puede crear una transferencia parcial de las habilidades entrenadas.

La supervisión reflexiva, práctica habitual en psicología clínica y trabajo social pero prácticamente inexistente en la formación policial española, consiste en sesiones periódicas en las que el agente revisa, con un supervisor formado, las intervenciones recientes que le han resultado difíciles o que no han tenido el resultado esperado. Este proceso de reflexión guiada permite al agente tomar conciencia de sus patrones automáticos de respuesta (los que no son visibles desde dentro de la intervención), identificar los momentos en que perdió el hilo de la desescalada y explorar alternativas que podrían haber funcionado mejor. La supervisión reflexiva no es una evaluación de rendimiento: es un espacio de aprendizaje seguro que requiere una cultura institucional de apertura y aprendizaje que no siempre existe.

Los programas de apoyo entre iguales (peer support programs), ampliamente desarrollados en los cuerpos policiales del norte de Europa y en aumento en los países anglosajones, forman a determinados agentes para proporcionar apoyo emocional informal a sus compañeros tras intervenciones especialmente exigentes. Este recurso ha demostrado reducir el estrés postraumático, el absentismo y el deterioro de la competencia comunicativa asociados a la acumulación de experiencias críticas sin procesamiento adecuado. La formación en comunicación de estos agentes de apoyo entre iguales incluye componentes específicos de escucha activa y regulación emocional que son directamente transferibles a la intervención con ciudadanos.

La evaluación de la competencia comunicativa policial plantea un desafío metodológico que la formación policial española no ha resuelto satisfactoriamente. Los exámenes escritos sobre conceptos de comunicación y desescalada tienen escasa validez predictiva sobre el desempeño real en situaciones de conflicto. La evaluación rigurosa requiere la observación directa del comportamiento del agente en situaciones simuladas o reales, la utilización de instrumentos de observación estructurada y la retroalimentación basada en conductas específicas y observables. Solo cuando la evaluación de la competencia comunicativa se incorpore de forma rigurosa a los sistemas de promoción y reconocimiento profesional, las instituciones policiales enviarán a sus agentes el

mensaje de que esta competencia es tan valorada como el dominio jurídico o la capacidad física.

CONCLUSIONES

La comunicación policial no es un conjunto de técnicas aplicables de forma mecánica: es una competencia compleja cuyo dominio requiere la integración de conocimientos neuropsicológicos, habilidades interpersonales entrenadas y una capacidad de autorregulación emocional que el propio agente debe cultivar de forma sistemática. Los avances de la neurociencia afectiva, la psicología del trauma y la investigación sobre justicia procedimental han transformado en los últimos veinte años nuestra comprensión de por qué determinadas formas de interacción generan escalada y otras la previenen. Sin embargo, estos avances no han permeado todavía de forma suficiente la cultura formativa de la Policía Local española.

El primer principio que se desprende del análisis realizado es que la desescalada eficaz comienza antes de que el agente hable: comienza en el estado de su propio sistema nervioso. Un agente que llega a una intervención con el sistema simpático dominante, el tono de voz elevado y la postura tensa, ya ha enviado señales de alarma al sistema nervioso del ciudadano antes de haber pronunciado una sola palabra. La regulación del estado interno del agente no es una concesión a su bienestar: es la primera herramienta operativa de la desescalada.

El segundo principio es que las técnicas de desescalada no son trucos retóricos: son aplicaciones prácticas de mecanismos psicológicos bien documentados. El etiquetado emocional reduce la activación de la amígdala. La escucha activa el sistema de participación social del ciudadano. El ofrecimiento de opciones restaura la percepción de agencia. La justicia procedimental en el trato construye legitimidad institucional a largo plazo. Comprender los mecanismos que subyacen a las técnicas permite al agente adaptarlas con criterio a situaciones nuevas, en lugar de aplicarlas como recetas rígidas que fallan cuando el contexto se aparta del ejemplo de libro.

El tercer principio es que la comunicación eficaz en situaciones de crisis no puede apresurarse. El tiempo, cuando la seguridad lo permite, es un aliado de la desescalada y no un enemigo de la eficiencia. La prisa para resolver una situación antes de que el ciudadano haya tenido la oportunidad de sentirse escuchado es una de las causas más frecuentes de escalada evitable. La tolerancia a la ambigüedad y la capacidad de sostener una situación tensa sin precipitar su resolución son competencias que deben entrenarse específicamente.

El cuarto principio es que la formación en comunicación policial no puede ser un módulo aislado en la academia: debe ser un proceso continuo que incluya práctica deliberada, retroalimentación de calidad, supervisión reflexiva y una cultura institucional que valore y reconozca la excelencia comunicativa como un marcador central de la profesionalidad policial.

Finalmente, la investigación sobre justicia procedimental demuestra que las consecuencias de la calidad comunicativa individual del agente trascienden con mucho la intervención concreta: se acumulan en la percepción colectiva de la legitimidad de la institución policial y determinan la disposición de la comunidad a colaborar con ella. La comunicación respetuosa, empática y eficaz del agente de Policía Local no es solo una cuestión de humanidad: es una condición de la eficacia policial a largo plazo.

BIBLIOGRAFÍA

Bowlby, J. (1969). Attachment and loss: Vol. 1. Attachment. Basic Books. Brehm, J. W. (1966). A theory of psychological reactance. Academic Press. De Shazer, S. (1985). Keys to solution in brief therapy. Norton.

Dreyfus, H. L., & Dreyfus, S. E. (1986). Mind over machine: The power of human intuition and expertise in the era of the computer. Free Press.

Ekman, P., & Friesen, W. V. (1978). Facial action coding system. Consulting Psychologists Press.

Ericsson, K. A., Krampe, R. T., & Tesch-Romer, C. (1993). The role of deliberate practice in the acquisition of expert performance. Psychological Review, 100(3), 363-406.

Figley, C. R. (1995). Compassion fatigue: Coping with secondary traumatic stress disorder in those who treat the traumatized. Brunner/Mazel.

Gilligan, J. (1997). Violence: Reflections on a national epidemic. Vintage Books.

Goleman, D. (1995). Emotional intelligence: Why it can matter more than IQ. Bantam Books.

Gross, J. J., & Thompson, R. A. (2007). Emotion regulation: Conceptual foundations. En J.

J. Gross (Ed.), Handbook of emotion regulation. Guilford Press.

Hall, E. T. (1966). The hidden dimensión. Doubleday. Ickes, W. (1997). Empathic accuracy. Guilford Press.

Lieberman, M. D., Eisenberger, N. I., Crockett, M. J., Tom, S. M., Pfeifer, J. H., & Way, B. M. (2007). Putting feelings into words: Affect labeling disrupts amygdala activity in response to affective stimuli. Psychological Science, 18(5), 421-428.

MacLean, P. D. (1990). The triune brain in evolution: Role in paleocerebral functions. Plenum Press.

Maslach, C., & Jackson, S. E. (1981). The measurement of experienced burnout. Journal of Occupational Behavior, 2(2), 99-113.

Miller, W. R., & Rollnick, S. (1991). Motivational interviewing: Preparing people to change

addictive behavior. Guilford Press.

Molis, J., & Noesner, G. (1997). Negotiating to save lives. *FBI Law Enforcement Bulletin*, 66(1), 1-7.

Ogden, P., Minton, K., & Pain, C. (2006). *Trauma and the body: A sensorimotor approach to psychotherapy*. Norton.

Porges, S. W. (2011). *The polyvagal theory: Neurophysiological foundations of emotions, attachment, communication, and self-regulation*. Norton.

Rizzolatti, G., Fatiga, L., Gallese, V., & Fogassi, L. (1996). Premotor cortex and the recognition of motor actions. *Cognitive Brain Research*, 3(2), 131-141.

Rogers, C. R. (1957). The necessary and sufficient conditions of therapeutic personality change. *Journal of Consulting Psychology*, 21(2), 95-103.

Siegel, D. J. (1999). *The developing mind: How relationships and the brain interact to shape who we are*. Guilford Press.

Tyler, T. R. (1990). *Why people obey the law*. Yale University Press.

Tyler, T. R. (2006). *Why people cooperate: The role of social motivations*. Princeton University Press.

Voss, C., & Raz, T. (2016). *Never split the difference: Negotiating as if your life depended on it*. HarperBusiness.

Weiner, B. (1986). *An attributional theory of motivation and emotion*. Springer.

VV.AA. (2023). *Guía de intervención policial en situaciones de crisis*. Ministerio del Interior, Secretaría de Estado de Seguridad. Gobierno de España.

Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. *Boletín Oficial del Estado*, núm.. 63, de 14 de marzo de 1986.

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. *Boletín Oficial del Estado*, núm.. 77, de 31 de marzo de 2015.

Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. *Boletín Oficial del Estado*, núm.. 313, de 29 de diciembre de 2004.

FUNDAMENTOS BÁSICOS PARA EL ANÁLISIS POLICIAL DE DISPOSITIVOS ELECTRÓNICOS



AUTOR/ES: FRANCISCO DE BORJA VIEJO ARENAL

FUNDAMENTOS BÁSICOS PARA EL ANÁLISIS POLICIAL DE DISPOSITIVOS ELECTRÓNICOS

Autor: Francisco de Borja Viejo Arenal

PRÓLOGO:

El siguiente documento, que lleva por nombre “FUNDAMENTOS BÁSICOS PARA EL ANÁLISIS POLICIAL DE DISPOSITIVOS ELECTRÓNICOS”, nace motivado por el creciente número de incidentes de seguridad que afectan cada vez más a los equipos electrónicos, según los datos publicados por el Ministerio del Interior, en el primer trimestre del año 2024, se registraron un total de 606.895 incidentes, de los que 484.467 (79,8% del total), son de tipo convencional, suponiendo un aumento del 0.9% respecto al mismo periodo del año anterior. El resto, 122.428 infracciones penales (20,2% del total) responden a ciberdelitos, suponiendo un aumento del 13.5% respecto al mismo periodo del año anterior. Al comparar, comprobamos como el aumento de la cibercriminalidad es superior al resto de delitos.

Para que seamos más conscientes, el mismo organismo publicó que en 2016, los ciberdelitos cometidos en el primer trimestre de ese año ascendieron a 70.178, mientras que, en el mismo periodo de 2023, llegaron a ser 427.448, lo que indica que, en solo ocho años, el cibercrimen ha sufrido un aumento superior al 509%.

La progresión seguirá en ascenso hasta el punto que, desde la plataforma Zerod, estiman que en 2025 los costes relacionados con los ciberataques podrían superar los 20.00 millones de euros.

Por todo esto, es necesario que los miembros de la FFCCSS tomen conciencia de la importancia de este tipo de criminalidad y se preparen para hacerle frente.

ÍNDICE

1. Introducción

- Concepto de informática forense
- Tipos de análisis forenses
- Objetivos de la informática forense
- Buenas prácticas
 - Plan de adquisición
 - Plan de análisis
- Estándares
 - The Forensics Process Model
 - The Abstract Digital Forensics Model
 - The Integrated Digital Investigation Model (IDIP)
 - Otros estándares

2. Fases del análisis forense
 - Preparación o estudio preliminar
 - Adquisición de datos
 - Adquisición de pruebas
 - Conservación
 - Análisis e investigación
 - Identificación de evidencias
 - Informe de conclusiones
 - Informe ejecutivo
 - Informe técnico
3. Clonación de dispositivos
 - Traditional Acquisition vs Live Response Acquisition
 - Procedimiento de clonación
4. Herramientas de Análisis Forense
 - Clasificación
 - Herramientas más utilizadas
5. Bibliografía.

INTRODUCCIÓN

Este capítulo tiene por finalidad dar a conocer qué es la informática forense, cuáles son sus objetivos, comprender las diferentes formas de recopilar pruebas y las buenas prácticas que se deben seguir.

Constituye una exposición de conocimientos teóricos básicos que deben asimilarse necesariamente, para posteriormente, poder asimilar el procedimiento práctico de análisis de dispositivos.

Concepto de informática forense

Cuando hablamos de informática forense, nos referimos a la investigación mediante la aplicación de un conjunto de procedimientos y técnicas científicas, analíticas y metodológicas, totalmente alejadas de la subjetividad, para identificar, recolectar, preservar, extraer, interpretar, documentar y presentar las evidencias obtenidas de infraestructuras tecnológicas, de manera que estas evidencias puedan ser aceptadas por un juzgado u órgano competente, durante un procedimiento, legal o administrativo, tras la comisión de un acto ilegal.

La función del analista no es valorar si los hechos son, o no, constitutivos de delito o infracción, la finalidad es mostrar e identificar a los receptores de la información, generalmente juristas sin conocimientos informáticos técnicos, las evidencias para que puedan tomar una decisión razonada.

Tipos de análisis forenses

El análisis forense no solo se utiliza para investigar delitos tecnológicos, también se utiliza para investigar delitos comunes en los que los autores hayan podido almacenar información en equipos informáticos.

En función del punto de vista al que hagamos referencia, nos podemos encontrar con distintos tipos de análisis forense. Según los sistemas analizados, nos encontramos con los siguientes tipos principales:

- **Análisis forense de sistemas:** es el más común, se encarga de analizar los incidentes de seguridad en los que los equipos afectados son aquellos que, en la actualidad, más se utilizan, incluyendo tanto estaciones de trabajo como servidores. Involucra analizar medios de almacenamiento, sistemas de archivos, memoria RAM y procesos de ejecución, por lo que hay que conocer las características de los diferentes sistemas operativos: Mac Os, Microsoft, sistemas Unix (Sun OS, SCO Unix, etc.) y sistemas GNU/Linux (Ubuntu, Debian, redHat, Fedora, etc.).
- **Análisis forense de redes:** se centra en el tráfico de los diferentes tipos de redes (cableadas, wireless y bluetooth...), para detectar actividades maliciosas o no autorizadas.
- **Análisis forense de sistemas embebidos:** rama cada vez más extendida, estudia los incidentes producidos en smartphones, tablet, PDA, etc. La estructura de los sistemas que forman este grupo, se asemeja mucho a la de un ordenador personal.

Si nos basamos en el ámbito en el que se lleva a cabo la investigación nos encontramos con dos tipos principales:

- **Investigaciones privadas:** en estos casos se lleva a cabo una investigación interna de una entidad privada, generalmente empresas. El objetivo inicial no es un proceso judicial, aunque podría derivar en él, lo que se pretende es realizar una auditoria por incidentes, sabotajes, espionaje industrial, malversación de recursos de la empresa, o disputas laborales. En estos casos hay que cumplir no solo con la legislación vigente, sino también con las políticas de la empresa, también es fundamental permitir la continuidad del negocio.
- **Investigaciones públicas:** este tipo de investigación se enmarcan dentro del ámbito judicial y son llevadas a cabo por las FFCCSS o por los propios organismos judiciales con finalidad jurídica.

Objetivos de la informática forense

Podríamos establecer como objetivo principal, el descubrimiento de evidencias legales para procedimientos judiciales. Estas evidencias son el conjunto de procesos y datos ejecutados en el equipo estudiado, que deben ser descubiertos y extraídos por el perito,

para un posterior análisis y verificación de su autenticidad.

Según Estrada (2010) *“la informática forense permite dar solución a problemas relacionados con la seguridad de la información, con el objetivo de salvaguardar la información digital, en el caso de haber ocurrido un delito, utilizando como medio al computador o algún equipo digital”*.

Otros objetivos destacables son:

- Esbozar procesos para asegurar que las pruebas digitales sean auténticas.
- Recuperar, resguardar y analizar el contenido digital.
- Recuperar los datos y documentos eliminados que sean de interés en un posible proceso judicial.
- Preservar las pruebas digitales, cumpliendo con una rigurosa cadena de custodia.
- Identificar ciberdelincuentes, descubriendo los motivos que los empujan a la comisión de los hechos delictivos.

Buenas prácticas

Al trabajar con evidencias, debemos asegurarnos que éstas no sean comprometidas, para ello se deben establecer una serie de pasos, entre los que se encuentra lo que se conoce como cadena de custodia (de la que hablaremos más adelante) y seguir cuidadosamente una serie de fases a la hora de llevar a cabo nuestra tarea, lo que nos permitirá garantizar que las pruebas no han sido modificadas, física o lógicamente, y mucho menos inventadas.

Se deben establecer una serie de pasos que nos permitan conservar las garantías de confiabilidad de una evidencia, ya que si no podemos asegurar que la evidencia no ha sido modificada y sufre cambios del estado original en el que se recogió, las conclusiones extraídas posteriormente de ella, no tendrán la validez suficiente al incluirlas en un proceso judicial.

Una buena práctica en cualquier actividad es la planificación, en nuestro contexto es fundamental, sobre todo en las fases de adquisición y análisis.

Plan de adquisición

Antes de iniciar la recolección de datos debemos tener claro que tecnologías se van a utilizar y que método de extracción vamos a seguir, todo deberá registrarse en el acto en nuestro cuaderno de bitácora.

Plan de análisis

En esta fase también debemos tener claro antes de iniciar el análisis, que tecnologías y

recursos se van a utilizar, reflejándolo nuevamente en nuestro cuaderno de bitácora, así como la hora de inicio y finalización de cada acto y el procedimiento seguido. También es interesante incluir una descripción del entorno de trabajo y adjuntar recursos audiovisuales.

Buenas prácticas

- Asegurar que personas no autorizadas puedan acceder a los dispositivos que se encuentren bajo peritación.
- Si el dispositivo está apagado, debe dejarlo apagado. En caso contrario, si está encendido, no debe apagarlo, además se debe desenchufar cualquier cable de red y apagar las conexiones Wi-Fi y Bluetooth o cualquier otro tipo de conexión
- Conocer la evidencia que se va a analizar, para poder prever qué tipo de equipo es el más adecuado para su manejo.
- Anotar absolutamente todo, como personas involucradas, pruebas, equipos, declaraciones, fechas u horarios.
- Reunir cualquier elemento al que se tenga acceso legal que se pueda convertir en evidencia

Estándares

La investigación forense, al considerarse una ciencia, posee estándares útiles para establecer las diferentes etapas de las que consta una investigación. En este apartado presentaremos una breve visión general de los modelos forenses más extendidos.

En los inicios, Kruse y Heise, establecieron los tres procesos básicos de toda investigación, estos son:

- Fase de adquisición de las evidencias.
- Fase de autenticación de las evidencias.
- Fase de análisis de las evidencias.

A partir de ahí fueron surgiendo otros modelos cada vez más completos

The Forensics Process Model

El Departamento de Justicia de Estados Unidos, publicó una guía que consistía en cuatro fases:

- Recogida: implica la búsqueda, reconocimiento y recolección de pruebas, así como su documentación.
- Examen: diseñado para facilitar la visibilidad de las pruebas, al tiempo que explica su origen y su significado. Implica revelar información oculta y oscura y la

documentación pertinente.

- **Análisis:** se tratará de estudiar las evidencias obtenidas en la fase anterior, determinando su importancia y valor probatorio para el caso.
- **Presentación de informes:** esto implica la redacción de un informe en el que se esbocen el proceso de examen y los datos pertinentes recuperados de la investigación general.

The Abstráct Digital Forensics Model

En esta ocasión se propone un proceso forense digital estandarizado que consta de nueve componentes:

- **Identificación:** tras el reconocimiento de un incidente, se determina su tipo basado en una serie de indicadores.
- **Preparación:** engloba la planificación de los medios que se utilizarán a lo largo del proceso, como son las técnicas, herramientas y órdenes de registro, además de las autorizaciones y apoyo a la gestión.
- **Estrategia de abordaje:** el objetivo de esta fase es aumentar lo máximo posible la recolección de pruebas no contaminadas, tratando que el impacto que sufra la víctima se el menor posible.
- **Preservación:** referido a las evidencias tanto digitales como físicas, engloba su aislamiento y seguridad.
- **Recopilación:** a través de procesos estandarizados y aceptados, se procede a la grabación y duplicado en el lugar.
- **Examen:** tras una búsqueda exhaustiva, detectar, de entre todas las pruebas disponibles, las que estén relacionadas con el hecho y puedan ser de utilidad.
- **Análisis:** el objetivo final es emitir conclusiones basadas en las pruebas encontradas, determinado la importancia de la información y la reconstrucción de fragmentos de datos.
- **Presentación:** engloba la exposición y explicación de las conclusiones.
- **Remisión de pruebas:** en esencia es asegurar que los indicios lleguen a los actores apropiados.

The Integrated Digital Investigation Model (IDIP)

Este modelo consta de cinco fases y fue desarrollado por Brian Carrier y Eugene Spafford:

- **Fase de preparación.**

- Fase de despliegue
- Fase de Investigación física del escenario del incidente
- Fase de investigación digital del crimen
- Fase de revisión

Las fases de Investigación de la escena física del crimen y de investigación digital del crimen, se dividen a su vez en seis subfases:

- Subfase depreservación
- Subfase de sondeo
- Subfase de búsqueda y recolección
- Subfase de presentación.

Por lo que el modelo organiza el proceso en cinco grupos que, en definitiva, componen 17 fases.

Otros estándares

Debemos recordar que estas normas, a pesar de ser de gran ayuda a la hora de ejercer una mejor práctica forense y elaboración de un peritaje informático, no son de obligado cumplimiento.

Tanto en el ámbito nacional como internacional, podemos encontrar un gran número de normas aplicables al análisis, preservación y recolección de evidencias informáticas, siendo algunas de las más destacados las siguientes:

Estándares a nivel nacional:

- UNE 197010:2015 “Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)”.

Norma que, publicada por AENOR, se encarga de establecer los requisitos formales que deben cumplir los informes periciales informáticos, sin establecer los métodos y procesos que se deben seguir tanto a la hora de elaborar dichos informes como en el aseguramiento de la escena, la recolección, la preservación o el análisis de las evidencias, teniendo como base la UNE 197001:2011, de “Criterios generales para la elaboración de informes y dictámenes periciales”, la cual es más genérica, ya que es aplicable a la realización de informes periciales de cualquier disciplina.

- UNE 71505:2013 “Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE)”. Esta norma, nuevamente publicada por AENOR, está compuesta por tres partes, la primera “Vocabulario y principios generales.”, la segunda “Buenas prácticas en la gestión de las evidencias electrónicas.” Y la tercera “Formatos y

mecanismos técnicos”.

En conjunto tratan de establecer el Sistema de Gestión de Evidencias Electrónicas (SGEE), los formatos que deben utilizarse a la hora de llevar a cabo los intercambios, los procesos que deben aplicarse para garantizar la confiabilidad, el sistema para gestionar la seguridad de las evidencias pudiéndolas integrar en el ciclo PDCA o ciclo de Deming.

- UNE 71506:2013 “Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.”

Esta norma completa la anterior, agrega términos, definiciones y abreviaturas y establece como actuar en cada una de las fases del proceso de análisis para garantizar que se cumpla con todos los requisitos legales.

Estándares a nivel internacional:

- ISO/IEC 27037:2012 “Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence”.

Esta norma viene a renovar las directrices establecidas en la norma RFC 3227 “Guidelines for Evidence Collection and Archiving”, ya que la ISO/IEC 27037:2012 establece la guía que debemos seguir para identificar, recolectar, adquirir y preservar las evidencias digitales en los dispositivos más modernos con las técnicas actuales.

- ISO/IEC 27042:2015 “Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence”

Esta norma nos guiará en el proceso de análisis e interpretación de las evidencias digitales estableciendo las directrices a seguir durante la actuación pericial.

FASES DEL ANÁLISIS FORENSE

El proceso de peritaje consta las siguientes etapas:

- Preparación o estudio preliminar
- Adquisición de datos
- Conservación
- Análisis o investigación

- Identificación de evidencias
- Informe de conclusiones

Preparación o estudio preliminar

En esta primera fase, se realiza un estudio inicial mediante la revisión de la documentación facilitada y las entrevistas al personal de la corporación que ha sido, o está siendo, afectada por el incidente, con el objetivo de tener una idea inicial del problema al que nos vamos a enfrentar.

Esta fase incluye la formación, mantenimiento de equipos, recursos, reciclaje, además de preparación específica en función del incidente a atender, debiendo recopilar tanta información como sea posible, por lo que podríamos decir, que esta fase se inicia incluso antes de la llegada del analista al lugar de los hechos.

Adquisición de datos

Esta segunda fase está destinada a la adquisición de datos e información esencial, recogidos tanto en la escena del incidente como en el laboratorio, en caso de ser necesario trasladar algún equipo involucrado. Esta etapa es una de las más críticas de todo el proceso, debido a que, en caso de cometer algún error, todo el análisis e investigación posterior podría ser invalidado, ya que podríamos no ser capaces de demostrar que la información recogida es la original. Un buen sistema para reducir este tipo de errores todo lo posible, es redactar un cuaderno de bitácoras a medida que vamos llevando a cabo el proceso.

Una de las primeras decisiones que deberemos tomar, es si proceder a apagar el equipo objeto de estudio o no. Esta decisión es de gran importancia ya que puede desembocar en pérdida de datos, sobre todo la información de la memoria volátil, los usuarios conectados, los procesos en ejecución o las conexiones de red existentes. Aunque más adelante lo desarrollaremos en profundidad, como primera aproximación podríamos decir que normalmente los equipos no deben apagarse, si existe riesgo de posible expansión de los daños al resto de equipos conectados a la red, debemos desconectarlo de dicha red, pero mantenerlo encendido.

En esta etapa se procede a la clonación o duplicado de los dispositivos afectados (que analizaremos más adelante). En caso de tener acceso a los equipos del atacante, habrá que tener mucho cuidado para evitar vulnerar sus derechos, lo cual podría derivar en la invalidación de las pruebas obtenidas.

Adquisición de pruebas

Como hemos mencionado, tras tener acceso al equipo, una de las primeras decisiones que deberemos tomar, es si proceder a apagar el equipo objeto de estudio o no, pudiendo proceder de diferentes modos:

- Apagar el equipo mediante el botón de alimentación (*Traditional Acquisition*).
- Apagar el quipo siguiendo el procedimiento de apagado normal (*Traditional Acquisition*).
- Mantener el sistema en funcionamiento (*Live Response Acquisition*).

Independientemente del método utilizado, la primera acción debe ser el aislamiento, tanto del sistema como de los datos relevantes, así como la congelación del estado del equipo estudiado, para conservar una imagen exacta.

El siguiente paso será la recopilación de toda la información necesaria, lo que incluye no sólo la información que contiene el equipo, también es importante recopilar toda aquella información relacionada con las interacciones de los diferentes agentes con el equipo estudiado, por lo que debemos entrevistarnos tanto con los administradores del sistema, como con el resto de usuarios que hayan tenido contacto con dicho sistema, lo cual no siempre será posible, debido a que podemos encontrarnos en una investigación encubierta, planeada y ejecutada para ocultar la identidad del autor.

Otros datos relevantes que debemos tratar de recopilar, son las contraseñas y toda aquella información sobre el sistema antes de iniciar el proceso de adquisición, ya que puede ahorrar tiempo y esfuerzo.

Una vez que el sistema está completamente aislado, el siguiente paso debe ser recoger toda la información posible no técnica, como los horarios de los usuarios que acceden al sistema, con lo que se puede crear una línea de tiempo que nos permita sospechar que se ha podido cometer un delito.

Durante la adquisición de la información anteriormente detalla y del análisis forense, existe una alta probabilidad de escribir accidentalmente en la unidad que contiene la evidencias. Dado que esto daría lugar a la no admisión de las pruebas en un juicio, debemos tener cuidado de no poner en peligro dicha evidencia. La forma más fácil de asegurarnos es usar un bloqueador de escritura.

Un bloqueador de escritura es un dispositivo que permite a un sistema leer datos de un dispositivo de almacenamiento, objeto de un análisis, al mismo tiempo que evita que cualquier comando de escritura realice una modificación no autorizada o formatee la unidad. Con este bloqueador se evita escribir a través de la interfaz del disco duro.

Este sistema constituye el mejor método de creación de imágenes forenses y el principal objetivo de su uso es obtener una imagen que no altere, de ninguna manera, dato alguno del dispositivo que está siendo objeto de estudio.

Existen dos tipos de bloqueadores de escritura, aunque ambos realizan la misma tarea:

- Por *software*, el cuál sustituye a una interfaz de acceso al disco duro en un equipo

con discos duros externos, funciona filtrando y bloqueando cualquier comando, de entrada o salida, enviado desde una aplicación a través de la interfaz de acceso, que pudiera modificar el disco duro. Una ventaja significativa de este tipo de bloqueadores, es que no necesita hardware adicional. La desventaja es que están limitados por las actualizaciones del Sistema Operativo.

- Por *hardware*, es un dispositivo de *hardware* portátil, fácilmente transportable, que se conecta físicamente al sistema informático. Su principal objetivo es interceptar y bloquear cualquier comando de modificación, antes de alcanzar el dispositivo de almacenamiento. Este tipo de bloqueadores funcionan de forma independiente, solventando la desventaja de los bloqueadores anteriores, además tiene indicadores más visuales para confirmar que no se está escribiendo en la unidad.

Como comentábamos anteriormente, para asegurar las evidencias es muy importante crear copias de los sistemas que van a ser foco de estudio, a los efectos de análisis.

Después de la adquisición física de los equipos, a través de la cadena de custodia, documentaremos tanto el incidente, como todas las acciones llevadas a cabo por los investigadores, documentando las evidencias y los dispositivos adquiridos durante todo el proceso

La cadena de custodia comienza en el momento en que el investigador forense entra en la escena del crimen, y continúa hasta el juicio, si lo hay, dando validez y solidez de las evidencias forenses del caso.

Podríamos definir la cadena de custodia como: “El procedimiento de validación, oportunamente documentado, que permite constatar la identidad, integridad y autenticidad de las evidencias, vestigios o indicios delictivos, desde que son encontrados y recogidos, hasta que se aportan al proceso como pruebas”. Básicamente, es tener todo documentado y bien identificado, para demostrar la no alteración de los artefactos recolectados y, en el caso de que haya una modificación, pueda ser identificada en tiempo y forma.

La evidencia tiene que ser transportada desde la escena del crimen al laboratorio forense para completar el proceso de adquisición. En el laboratorio, las pruebas deben de almacenarse de forma segura.

Hay que tomar ciertas precauciones para asegurarse de que la evidencia llega sin ningún daño o alteración, utilizando envases sin electricidad estática donde introducir las evidencias, sellar el paquete y firmar el sello.

Si alguien no autorizado intenta abrir el paquete, el sello se rompería y se estropearía la firma, invalidando la prueba. Cada vez que alguien necesite acceder a los datos, el paquete debe ser puesto en un nuevo paquete y el nuevo paquete debe ser sellado y

firmado.

Esto es especialmente importante en aquellos casos que, inevitablemente, se posponen varias veces, pudiendo dilatarse la duración del proceso por varios años. Por lo que es imprescindible evitar el deterioro de las evidencias.

DIARIO DE INVESTIGACIÓN O CUADERNO DE BITÁCORAS

Es un elemento común en todas las investigaciones.

Se utiliza para ir anotando inmediatamente todos los pasos que se van llevando a cabo, para reunir y preservar las evidencias, mostrando el proceso real de investigación.

Es recomendable organizarlo por días, desde el primero hasta el fin del proceso, pero no existe un sistema estandarizado para organizarlo.

Las notas nos permitirán calcular de forma precisa la gravedad del incidente, evitando estimaciones exageradas, registrando los hechos acontecidos, las impresiones del analista y todo aquello que le resulte relevante.

Conservación

En esta etapa se debe garantizar la información recopilada, con el fin de garantizar que en absoluto se destruyan o transformen indicios, evidencias y pruebas.

Uno de los principales problemas a los que se enfrenta el informático forense, es el de poder demostrar que las evidencias digitales incautadas por el profesional, son exactamente las mismas que las que se trasladan a la autoridad competente. Por ello, la cadena de custodia, es uno de los pilares fundamentales de esta fase y, en general, de todo el ámbito del peritaje informático. Mantener la integridad de las pruebas digitales es crucial para garantizar su validez y evitar cualquier tipo de contaminación que pueda comprometer su fiabilidad. Debido a que, tras concluir todo el proceso de análisis, debemos corroborar que los datos se mantuvieron sin ningún tipo de alteración.

La cadena de custodia de una prueba digital, es el procedimiento de informática forense, meticulosamente documentado de forma cronológica, que permite constatar el origen y garantizar la identidad, autenticidad e integridad del elemento digital, desde que es encontrado e intervenido, posteriormente analizado y finalmente presentado.

Durante todo el proceso, se debe cumplir con una serie de requisitos, técnicos y jurídicos, que aseguren la autenticidad e inalterabilidad de las pruebas, protegiéndolas de cualquier manipulación o alteración. Las pruebas irán pasando por diferentes etapas bien descritas, cada una representada por las personas que manejan la evidencia, los traslados -indicando las horas y posibles incidentes que pudieran surgir durante los mismos-, los métodos utilizados para su obtención y el tratamiento que recibe hasta su uso en el proceso judicial, quedando las evidencias perfectamente identificadas. En cada

cambio de posesión se debe anotar quien, como, donde y cuando recibe y entrega la evidencia, así como las medidas de custodia y preservación de la misma. Quien se haga cargo de las evidencias también lo hará de la cadena de custodia.

Según Domínguez (2013) “una vez asegurada la cadena de custodia, aquí, empieza el trabajo verdadero del perito forense”.

El Tribunal Supremo define la cadena de custodia como «el conjunto de actos destinados a la recogida, traslado y conservación de los indicios o vestigios obtenidos durante una investigación criminal».

Por su parte, la Sala Segunda del Tribunal Constitucional, concretamente en su sentencia 170/2003 del 29 de septiembre de 2003, establece los requisitos que deben cumplirse, en los casos penales con control judicial, para garantizar la cadena de custodia de los elementos informáticos incautados:

- Describir el material informático intervenido.
- Proceder al bloqueo y precinto de cualquier ranura o puerto del ordenador en presencia del Letrado de la Administración de Justicia.
- Evitar el deterioro o manipulación de las evidencias, llevando a cabo la custodia en un lugar adecuado.
- Hacer constar la cadena de custodia en la causa.
- Garantizar el derecho a un proceso con todas las garantías que asegure la validez de la prueba, para ello es necesario que exista control judicial durante la recogida y custodia de la prueba.

Análisis e investigación

El siguiente paso consiste en analizar, indexando los datos anteriormente adquiridos, con el objetivo de comprender la información para su posterior estudio.

En esta fase, el analista tiene a su disposición varias herramientas, pero las más utilizadas son “EnCase® Forensic” (<https://www.opentext.com/es-es/productos/encase-forense>) disponible para sistemas operativos Windows y “The Sleuth kit & Autopsy” (<https://www.sleuthkit.org/autopsy/>) disponible para sistemas GNU/Linux, siendo ambos capaces de analizar sistemas Unix, Linux, Mac OS y Microsoft.

Una de las primeras decisiones será determinar la configuración horaria del sistema, pudiendo validar de esta forma, las fechas y horas de todas las acciones que llevemos a cabo, evitando así, que nuestra investigación pueda ser cuestionada con un contraperitaje. Tras esto, podremos realizar el estudio de la línea de tiempo (timeline) y determinar todas las acciones llevadas a cabo en el equipo, desde su puesta en marcha, hasta el momento de clonación del disco.

La información analizada se encuentra en varias fuentes:

- Registros de los sistemas analizados.
- Registro de los detectores de intrusión
- Registro de los cortafuegos
- Ficheros del sistema analizado: Se debe actuar con precaución al analizar las carpetas personales de los usuarios, las cuales se encuentran en el directorio /home en sistemas GNU/Linux y en c:\documents and settings\ en sistemas Windows.

Identificación de evidencias

En esta etapa, el analista se encargará de destacar qué información es la relevante para el incidente investigado, de entre toda la amalgama de datos adquiridos y analizados.

Informe de conclusiones

La última fase es la generación del informe de conclusiones o informe pericial, en este documento se detallarán todas las actividades del proceso de investigación y las conclusiones obtenidas, basadas en la información recopilada. Realmente no se trata de un solo informe, si no de dos, uno denominado Informe técnico y un segundo denominado Informe ejecutivo

En ciertas situaciones se pueden unificar en uno solo, el cual tendría una parte técnica y otra ejecutiva, aunque esta práctica no es recomendable.

La redacción de los correspondientes informes es una tarea tediosa y compleja, ya que se debe plasmar todas las evidencias, indicios y pruebas recopiladas, el método aplicado -tanto para la recolección como para el análisis-, las herramientas utilizadas, la fecha de finalización, las personas involucradas en su desarrollo y toda aquella información relevante. Además, debe redactarse de manera clara y rigurosa, explicando minuciosamente cada punto.

Informe ejecutivo

Este informe está dirigido a los altos cargos de las empresas, los cuales no suelen tener conocimientos técnicos de informática, por lo que se debe utilizar un lenguaje lo menos técnico posible, expresarse de una manera clara y sencilla para que pueda ser fácilmente comprendido, pero sin dejar de ser riguroso. Si no se puede evitar el uso de algún término técnico, éste debe ser explicado.

Este informe debe estar compuesto al menos por los siguientes puntos:

- I. Introducción: Detallaremos el impacto económico sufrido por la empresa y el objeto del informe.

- II. Descripción: Donde se detalla el incidente en sí.
- III. Recomendaciones: Recoge las acciones que debe llevar a cabo la entidad, para evitar que el incidente se vuelva a producir.

Informe técnico

En esta ocasión el público al que va dirigido son personas con altos conocimientos técnicos de informática. Este informe debe estar compuesto al menos por los siguientes puntos:

- I. Introducción: Se describe el objeto del informe y cada uno de los apartados que los componen.
- II. Preparación del entorno y recogida de datos: desarrolla el procedimiento seguido para la configuración del entorno forense, la adquisición y verificación de las imágenes del equipo objeto de estudio.
- III. Estudio forense de las evidencias: Descripción de todo lo adquirido y analizado, y de lo que representa.
- IV. Timeline: Permite controlar la visualización de la cadena de acciones realizada por la amenaza a lo largo del tiempo
- V. Conclusiones: Argumentadas detalladamente tras la realización del análisis.

CLONACIÓN DE DISPOSITIVOS

Antes de comentar la forma en la que se lleva a cabo la clonación de los dispositivos para su posterior análisis, vamos a indicar las diferencias, ventajas e inconvenientes entre la adquisición de un equipo encendido (***Live Response Acquisition***) y la adquisición de uno apagado (***Traditional Acquisition***).

Traditional Acquisition vs Live Response Acquisition

La probabilidad de que los investigadores modifiquen los datos de una evidencia es muy grande, por ello, se deben tomar suficientes precauciones para asegurarse de que el ordenador no permita ninguna modificación durante el proceso de copia, del original o la imagen copiada del disco duro original. Para ello, como se ha comentado con anterioridad, podemos utilizar los bloqueadores de escritura.

La diferencia más importante entre la adquisición forense de un sistema en vivo y uno apagado es que, una vez que el sistema se apaga, se pierde toda la información volátil alojada en la memoria RAM, no pudiendo ser recogida toda esa información, a veces determinante.

Estudiar un equipo mediante el sistema de análisis de equipos apagados (***Traditional Acquisition***), lleva asociada una serie de dificultades a la hora de realizar el estudio

forense del equipo, entre las que podemos destacar las siguientes:

- Cada vez está más extendido el uso de la criptografía. Obtener un equipo cuya información se encuentre cifrada, supone un grave inconveniente, ya que, aunque se consiga la imagen completa del disco bit a bit, al encontrarse la información cifrada, ésta no tiene ningún valor práctico, ya que la unidad solo puede ser descifrada con una contraseña única. No solo los criminales utilizan esta técnica para ocultar sus actos, también es utilizada en algunos sistemas operativos.
- Adquisición de los datos de red, como puertos, conexiones establecidas, etc. Este tipo de información es volátil y se pierde en el caso de que se desconecte el ordenador.
- Todos los datos deben ser recogidos y examinados como evidencias. Sin embargo, actualmente se dispone de sistemas con grandes capacidades de almacenamiento, por lo que, esa cantidad de información debe ser analizada, requiriendo mucho tiempo. Los archivos de registro también tienden a aumentar de tamaño y dimensión, lo que complica la investigación.
- Falta de procedimientos estandarizados en los que se recopilan datos sin valor, que consumen un tiempo innecesario.
- A veces, los equipos objeto de estudio son sistemas que no pueden ser apagados debido a que pertenecen a empresas en las que, para su funcionamiento, es necesario que los sistemas se encuentren constantemente encendidos y funcionando.
- Es importante que los investigadores estén equipados con herramientas y mecanismos validados para que puedan realizar la adquisición correcta y validada, con la finalidad de que los datos obtenidos se puedan ver como evidencia y admisibles en un juicio.
- No se podrán recoger los datos volátiles como los almacenados en la memoria RAM.

Por todo lo anterior, la adquisición forense en vivo suele ser la mejor alternativa, ya que nos permitirá acceder a mucha de información de gran valor que se habría perdido en el análisis forense tradicional.

El análisis en vivo (***Live Response Acquisition***) nos permitirá recuperar información volátil del equipo estudiado, acceder de un modo más sencillo al resto de la información almacenada en el sistema, permitir la continuidad funcional de la empresa y limitar la cantidad de datos a almacenar. Ya que, en muchas ocasiones, de toda la información disponible, solo parte de esta nos resultará valiosa para los hechos objeto de investigación.

Todo lo anterior soluciona parte de los inconvenientes del sistema tradicional, lo que está provocando que este tipo de análisis sea cada vez más habitual en la informática

forense.

Aun así, este tipo de adquisición presenta una serie de inconvenientes:

- El investigador debe tener conocimientos suficientes de la amplia variedad de sistemas *hardware*, *software* y sistemas operativos. Ya que, aunque hay muchos componentes y aspectos comunes, los sistemas se pueden configurar de diferentes formas.
- Durante el proceso de adquisición de datos del sistema sospechoso, es muy fácil modificar la información recogida. Si estos datos son alterados, las evidencias descubiertas podrían ser desestimadas en un proceso judicial. Parte de la adquisición en vivo ejecuta código en la CPU del sistema, lo que puede alterar los datos en los registros de la CPU, la memoria RAM o el disco duro. Además, en algunas ocasiones, no es posible utilizar bloqueadores de escritura, lo que favorece aún más la modificación de la información.
- En el mercado podemos encontrar una serie de herramientas antiforenses, disponibles en diferentes plataformas, las cuales pueden destruir el contenido del equipo cuando el sistema operativo detecta un programa de adquisición forense. Algunos de estos programas son Evidence Eliminator, The Defiler's Toolkit, Diskzapper, CryptoMite, Tracks Eraser Pro e Invisible Secrets.
- Un sistema encendido, podría permitir tanto el acceso remoto al sistema, posibilitando la modificación de datos, volviéndolos inservibles ante los tribunales, como el borrado de la información que contenga el equipo objeto de estudio.
- Por último, en algunos casos se recopilan una cantidad limitada de información. Esto no siempre puede constituir una representación completa del sistema original afectado y puede ser interpretado como una posible alteración de los datos.

Tradictional acquisition

El análisis de adquisición de un sistema apagado, a menudo se denomina método digital tradicional o Traditional Acquisition.

La adquisición en un sistema apagado, en caso de encontrarlo encendido, implica quitar la corriente eléctrica al sistema, impidiendo que en él se ejecuten procesos maliciosos y se eliminen datos. Como ya ha sido comentado, al apagar el equipo se perderá toda la información volátil, por ello, un paso previo al corte del suministro, es recopilar toda esta información volátil creando una instantánea de los archivos swap y de la información del sistema, tal y como se encontraba antes de apagarse por última vez.

Podríamos definir este tipo de análisis como “el realizado en un ordenador apagado” y dividir el estudio en cuatro etapas:

- **Recolección de evidencias:** llevada a cabo en el lugar del incidente y se basa en la búsqueda y adquisición de información. Las principales acciones son la duplicación de discos y la recogida de pruebas al azar, como son CDs, entrevistas personales, etc.
- **Examen de la información:** basado en la investigación de los datos adquiridos. Esta etapa tiene como objetivo identificar y extraer los datos pertinentes al caso específico, e incluye el análisis del sistema de archivos y la extracción de las evidencias.
- **Análisis:** proceso de utilización de los datos, para demostrar las acciones realizadas en el equipo. Esta etapa consiste en la navegación, la consulta y la correlación de datos existentes.
- **Notificación:** es la última etapa, en ella se expone, de una forma escrita, la información recopilada mediante los informes técnicos y ejecutivos.

El esquema que debe seguir el investigador es el siguiente: tras llegar al lugar, determinar si el equipo está encendido o apagado. En caso de estar encendido hay que apagarlo, bien de forma brusca, bien siguiendo el procedimiento habitual de apagado del sistema, pero se recomienda el apagado brusco desconectando el equipo directamente de la red. Una vez apagado el equipo hay que sacar el disco duro y añadirlo, como unidad externa, al sistema forense. El siguiente paso sería copiar el contenido del disco, devolviendo el disco al sistema original o preservarlo como evidencia introduciéndolo en una bolsa antiestática para evitar posibles daños. Durante el proceso, se deben tomar todas las medidas necesarias para garantizar que no se modifican los datos.

Éste es un procedimiento fácil de seguir, siendo, durante muchos años, el único medio para llevar a cabo adquisiciones forenses.

Live response acquisition

El método de adquisición forense en vivo (*Live Response Acquisition*) es similar al anterior. Se desarrolló en respuesta a las deficiencias de las técnicas de adquisición forense tradicionales, con la intención de no perder los datos volátiles y facilitar el acceso a los archivos cifrados.

Como en el caso anterior, el objetivo es conseguir las evidencias necesarias garantizando que la información permanezca inalterada.

Las etapas seguidas en este caso, son las mismas que en el sistema tradicional: recolección de evidencias, examen de la información, análisis y notificación. La única excepción que debemos reseñar, es que, en esta ocasión, se deben utilizar medios para captar y almacenar la información volátil.

El esquema que debe seguir el investigador es el siguiente: tras llegar al lugar, determinar si el equipo está encendido o apagado. En caso de estar apagado, seguirá el

procedimiento de adquisición forense de un sistema apagado o tradicional. En caso de estar encendido, el primer paso será decidir si los datos se copiarán a nivel local, o a través de la red. Lo siguiente será garantizar que no se modificarán los datos durante la extracción, por lo que conectará un bloqueador de escritura, tanto en el equipo investigado como a la unidad externa al sistema forense, para copiar el contenido del equipo objeto de estudio.

No hace falta indicar que, en caso de estar iniciada la sesión o no encontrarse su inicio protegido, el proceso de investigación será bastante más sencillo. Siendo aún mejor si la sesión cuenta con derechos de administración. Si la cuenta actual no cuenta con derechos administrativos, la funcionalidad del usuario con la que el investigador puede trabajar, dependerá de los derechos asignados a la cuenta actual y el software instalado.

Otro detalle a tener en cuenta es si dicha cuenta se encuentra en un entorno real o virtual, ya que, aunque utilizaremos el mismo método de investigación en los diferentes entornos, si la sesión se ha iniciado en una máquina virtual, deberemos hacer un análisis más detallado ya que en este caso deberemos recopilar información del sistema anfitrión y de todas las posibles máquinas virtuales que éste aloje. En este caso tendremos que utilizar una serie de técnicas, las cuales nos indicarán si el sistema es real o virtual.

La más sencilla de todas ellas es la búsqueda de:

- Notas de los derechos de autor o cadenas de los proveedores en varios archivos.
- Los controladores de *hardware* específicos de las máquinas virtuales.
- BIOS específico de las máquinas virtuales.
- Direcciones MAC específicas de las máquinas virtuales.
- Herramientas de las máquinas virtuales instaladas.
- La virtualización por *hardware*.

Debemos tener presente que toda esta información es fácilmente modificable, por lo que le daremos la importancia precisa.

Un método más fiable consiste en revisar las características del hardware. Para el caso de los sistemas operativos Microsoft, tenemos disponible la herramienta de línea de comandos DevCon, que muestra información detallada sobre los dispositivos en equipos que ejecutan Windows, muy útil en la detección del hardware que se encuentra en el sistema, identificando cualquier hardware de la máquina virtual, en algunos casos los discos IDE se denominan “HD virtual”.

Otra técnica que nos ofrece fiabilidad es la instalación de detectores de máquinas virtuales, teniendo en cuenta que este *software* puede tener un impacto negativo sobre

la solidez de la evidencia forense. Algunas de estas herramientas son Red Pill, Jerry, ScoopyNG y VMware *Virtual Machine Detector*.

Procedimiento de clonación

Como ya se ha mencionado, a la hora de extraer evidencias de los sistemas investigados, no debemos trabajar directamente con los datos originales, por lo que tendremos que generar copia de dichos datos. El método más utilizado es la clonación de discos, que consiste en copiar todo el contenido de un disco duro, bit a bit, en otro dispositivo de almacenamiento o fichero de imagen, durante el proceso se obtiene la firma hash de los bits leídos. Con este método obtendremos una copia exacta, a bajo nivel, del elemento de almacenamiento, permitiéndonos también acreditar que el contenido original coincide con el duplicado, debido a que la firma hash de ambos es la misma. Para validar la cadena de custodia, la firma hash del dispositivo utilizado como destino y la del dispositivo original, deben coincidir. En el caso que varíe un solo bit durante el proceso de clonado, no se podría garantizar que la prueba no ha sido alterada, por lo que la cadena de custodia sería inválida.

Para evitar que las pruebas no sean admitidas y garantizar la integridad de la cadena de custodia, es imprescindible que el perito informático documente de forma exhaustiva todo el proceso de clonado, haciendo constar la situación, tipología y características, tanto del dispositivo original intervenido, como del que utilizará para volcar la información clonada. Es evidente que todo esto se incluirá en el informe de peritaje, de forma clara, detallada y fácilmente comprensible, con la finalidad de poder certificar la validez de la cadena de custodia de las evidencias digitales intervenidas, tanto físicas como lógicas, antes de proceder al estudio de las mismas.

Se deben realizar al menos tres copias, por si surge algún error en uno de ellos, podamos trabajar con otra copia y no perder información. Los discos utilizados para almacenar la copia deben ser nuevos o previamente formateados a bajo nivel para garantizar que no queden impurezas que provoquen la invalidez del estudio. Tras realizar el clonado, los discos deben ser etiquetados y precintados.

En el mercado hay disponibles gran cantidad de herramientas de clonado gratuitas o no. Podemos mencionar Clonezilla, Rescuezilla, GParted, DrivelImage XML, Redo Rescue, Acronis Disk Director, Paragon Drive Copy Professional, AOMEI Backupper, EaseUS Todo Backup o Macrium Reflect.

HERRAMIENTAS DE ANÁLISIS FORENSE

Clasificación

Podemos diferenciar dos grandes grupos:

- Herramientas de hardware como clonadoras, bloqueadores de escritura o capturadoras de tráfico de red.
- Herramientas de software, utilizadas principalmente en la fase de análisis de las pruebas, éstas, a su vez, podemos clasificarlas según el tipo de análisis a realizar:
- Análisis forense de red: orientado a la monitorización y análisis del tráfico de las redes de datos, se utilizan herramientas de captura de tráfico de red para su análisis posterior. Este tipo de análisis no solo nos permite detectar el origen y destino de los paquetes de red, también podemos identificar la información que contienen. Al tratarse de información dinámica y volátil, la investigación debe tener un carácter proactivo. *Ejemplos: Wireshark, tcpdump, NetworkMiner...*
- Análisis forense de memoria: nos permitirá almacenar en un archivo el contenido de la memoria volátil, para, posteriormente, llevar a cabo el análisis (lo que en esencia es un volcado de memoria), de esta forma podremos averiguar los ficheros temporales que se estaban utilizando, qué procesos estaban activos, las librerías que se habían cargado, etc., pudiendo identificar las evidencias no visibles en el disco duro. *Ejemplos: Volatility, BlackLight, Rekall...*
- Análisis forense de equipos: en esta ocasión se lleva a cabo el análisis de sistemas completos, sobre todo de las unidades de almacenamiento (disco duro, sólido, etc) además de los registros del sistema o los procesos abiertos en servidores, equipos de sobremesa, ordenadores portátiles y tabletas. Son útiles para identificar ficheros eliminados, ocultos o modificados. *Ejemplos: EnCase, FTK, Autopsy, Bulk_extractor...*
- Análisis forense de malware: se trata de herramientas que emplean técnicas de ingeniería inversa para detectar la presencia de *malware* en un dispositivo, conocer su comportamiento y capacidades, así como para evaluar los daños potenciales y/o producidos y determinar su autoría. *Ejemplos: Cuckoo Sandbox, OllyDbg, IDA Pro, Radare2...*
- Análisis forense de logs: permiten examinar los archivos de registro generados por sistemas, aplicaciones y dispositivos para encontrar evidencias de actividades maliciosas, violaciones de seguridad o problemas operativos, permitiendo establecer una línea temporal, donde queden reflejados los comportamientos maliciosos a lo largo de dicha línea temporal. *Ejemplos: Splunk, ELK, Logtail...*

Herramientas más utilizadas

- Encase® Forensic: una de las herramientas comerciales de análisis forense más utilizadas en el mundo, propiedad de la empresa Guidance Software, considerado un estándar en el análisis forense de sistemas. Ofrece una amplia gama de características y capacidades para la adquisición y análisis de evidencia digital, como son: adquisición de imagen forense, análisis avanzado de archivos, análisis de registro y actividad, análisis

de dispositivos móviles, análisis de nube y análisis de memoria. (<https://www.opentext.com/es-es/productos/encase-forense>)

- The Forensic ToolKit: software comercial [de análisis forense informático](#) para plataformas Windows, propiedad de Exterro, pero desarrollado originalmente por [AccessData](#), recopila datos de cualquier dispositivo o sistema digital y realiza el análisis forense de los mismos. (<https://www.exterro.com/digital-forensics-software/forensic-toolkit>)
- FTK Imager: herramienta forense digital gratuita desarrollada por AccessData muy útil en la investigación forense digital, ya que permite crear imágenes forenses de dispositivos de almacenamiento, como discos duros, dispositivos USB o tarjetas de memoria, entre otros. Actualmente propiedad de Exterro (<https://www.exterro.com/digital-forensics-software/ftk-imager-temp>)
- The Sleuth kit & Autopsy: “The Sleuth kit” es un conjunto de herramientas de análisis forense de código abierto, que se utiliza para examinar discos duros y medios extraíbles con el fin de buscar y analizar datos digitales, cuyo autor es Brian Carrier. Inicialmente fue desarrollada para plataformas UNIX, pero actualmente también se encuentra disponible para OS X y Windows. El código que utiliza es el mismo que el de [The Coroner’s Toolkit](#) (TCT), [Wietse Venema](#) y Dan Farmer.

Este ToolKit puede funcionar conjuntamente con “Autopsy”, consistente en una interfaz gráfica que agrupa

todas sus herramientas y plugins (<https://www.sleuthkit.org/>)

- Volatility Framework: framework de código abierto bajo licencia GNU (General Public License), creado por Aaron Walters, está escrito en python y se enfoca principalmente en el análisis forense de memoria, su uso más extendido es en los casos de respuesta a incidentes y el análisis de malware. El desarrollo de Volatility está soportado por The Volatility Foundation, organización sin ánimo de lucro. (<https://volatilityfoundation.org/the-volatility-framework/>)
- Wireshark: se trata de un analizador de protocolos open-source, disponible tanto para plataformas Unix como Windows. Principalmente se utiliza para el análisis del tráfico de red, pero también destaca en la resolución de problemas de red y el estudio de las comunicaciones. Esta herramienta tiene disponibles gran variedad de filtros que nos permiten, de forma fácil, establecer criterios de búsqueda aplicables a los protocolos que soporta, en la actualidad más de 1100.

Wireshark presenta una interfaz intuitiva y sencilla que permite visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando al administrador gestor de las redes, una multitud de posibilidades,

llegado el momento de afrontar trabajos en el análisis del tráfico de datos.
(<https://www.wireshark.org/>)

- Scalpel: herramienta libre de código abierto para sistemas operativos Linux, destinado a la recuperación de datos, permite al investigador recuperar archivos borrados y fragmentados de discos duros y otros medios de almacenamiento.
- OSForensics: desarrollado por passmark software, proporciona una de las formas más rápidas y poderosas de localizar archivos en un equipo que disponga de sistema operativo Windows. Nos permitirá realizar búsqueda filtrando por criterios como tamaño, nombre, fecha de creación y modificación, entre otros. Los resultados se devuelven presentándose en varios tipos de vistas. Esto incluye la Vista de línea de tiempo, que permite examinar las coincidencias en una línea de tiempo, haciendo evidente el patrón de actividad del usuario en la máquina.
(<https://www.osforensics.com/>)

BIBLIOGRAFÍA.

<https://www.incibe.es/>

<https://www.ra-ma.es/>

<https://www.uoc.edu/es>

<https://www.foc.es/>

<https://andaluciavuela.es/>

<https://www.comunixgroup.com/>

<https://www.coursera.org/>

LA INTEGRACIÓN DEL BASTÓN EXTENSIBLE EN LA POLICÍA LOCAL. METODOLOGÍA, CONOCIMIENTO Y CRITERIOS.



AUTOR: JACOB PICHARDO PÉREZ

LA INTEGRACIÓN DEL BASTÓN EXTENSIBLE EN LA POLICÍA LOCAL. METODOLOGÍA, CONOCIMIENTO Y CRITERIOS

Autor: Jacob Pichardo Pérez

EPÍLOGO

En la actualidad es de vital importancia el conocimiento del material de trabajo que vamos a utilizar en nuestra jornada laboral como Policías Locales. Es por ello que desde esta publicación vamos a centrarnos en todo lo que acontece al uso y conocimiento del bastón extensible policial.

El presente LA INTEGRACIÓN DEL BASTÓN EXTENSIBLE EN LA POLICÍA LOCAL. METODOLOGÍA, CONOCIMIENTO Y CRITERIOS, se ha publicado en colaboración con el Sindicato Independiente de Policía de Andalucía Sip-an, para ser entregado en su versión Libro a los alumnos de las distintas Acciones Formativas de perfeccionamiento en ésta materia y en su versión de Publicación Electrónica, ha sido publicada en el Área de Formación – Biblioteca Virtual - Publicaciones de Interés Policial www.sip-an.es, del citado sindicato.

ÍNDICE

- CARACTERÍSTICAS DE LA DEFENSA EXTENSIBLE
- FUNCIONAMIENTO DE LA DEFENSA EXTENSIBLE
- DIFERENTES TIPOS DE DEFENSAS EXTENSIBLES
- MANTENIMIENTO DE LA DEFENSA EXTENSIBLE
- FUNDAS PARA LA DEFENSA EXTENSIBLE
- ACCESORIOS PARA LA DEFENSA EXTENSIBLE
- APERTURA Y CIERRE DE LA DEFENSA EXTENSIBLE
- LUGAR DE PORTE DE LA DEFENSA EXTENSIBLE
- MANEJO BÁSICO DE LA DEFENSA EXTENSIBLE
- ZONAS DE IMPACTO CON LA DEFENSA EXTENSIBLE
- BIBLIOGRAFIA

CARACTERÍSTICAS DE LA DEFENSA EXTENSIBLE

El concepto de defensa extensible se ideó en Oriente, donde sus primeros modelos se caracterizaron por ser muy simples y básicos en lo que se refiere a su diseño y métodos de construcción.

En los años 70 se ideó el primer modelo americano de defensa extensible, al que se le llamó “Titan Taper”, el cual no tuvo mucha repercusión al dejar claro que tanto el método de construcción como su durabilidad, no fueron compatibles con el uso policial para largos periodos de tiempo.

Las defensas extensibles policiales de la actualidad están consideradas como armas no letales o de baja letalidad, las cuales están diseñadas para un uso defensivo en situaciones operativas, y ofrecen un fácil porte debido a su bajo perfil. Debido a su adecuado porte, estas defensas ofrecen grandes ventajas para aquellos Policías Locales que realizan servicios hasta de paisano. Del mismo modo y en función de sus características, este tipo de defensas extensibles facilitan una rápida extracción y son fácilmente portables en cualquier tipo de servicio o cometido, sin necesidad de tener que dejarlas en ningún momento dentro del patrullero o en la jefatura.

Este tipo de defensas extensibles suelen estar compuestas en su interior por tres shafts telescópicos, los cuales se bloquean por la fricción (en relación al modelo de defensa mas extendido en el mundo policial) que produce el Policía al extender el brazo para proceder a su apertura. Estos shaft pueden venir en varios colores, los más usuales son en color negro o gris, independientemente de su material, ya sea este de acero o aluminio. Desde esta publicación se recomienda adquirir la defensa extensible con los shafts de color negro, así a simple vista o de cara a cualquier tipo de grabación, no parece tan agresiva, ya que el color gris a simple vista delata que esta misma es de material rígido (acero o aluminio).

Existen diferentes materiales con los que se suelen fabricar las defensas extensibles, normalmente podemos hacer dos grandes grupos en lo que se refiere a sus materiales de construcción, estos son: las defensas de aluminio o acero y las defensas de polímero. Las defensas de polímero tienen el gran inconveniente que todas son susceptibles de romperse, ya que su material de fabricación no es para nada seguro cuando hablamos en términos de uso de la fuerza. No debemos de olvidar que la defensa extensible será en todo momento considerada como un arma de baja letalidad o no letal, por lo que cuando el Policía Local haga uso de ella será porque exista un concreto peligro hacia su persona o para terceros. Dicho esto es de lógica común que cuando el Policía Local use la defensa será necesario en la mayoría de los casos de aplicar la misma con fuerza o cierta presión, todo ello con la finalidad de conseguir la obediencia deseada o la incapacitación por parte del sujeto agresivo. Por todo ello no deberíamos de priorizar el uso de aquellas defensas que sean tendentes a romperse con cierta facilidad cuando se le aplica la fuerza, ya que en este caso estaríamos ante una gran desventaja y por tanto tendríamos que solventar el problema que nos acontece en el momento menos indicado, debido a que no podremos hacer uso de esta herramienta durante la actuación en cuestión.

Debido a ello desde esta publicación se aconseja en todo momento la adquisición de defensas extensibles que estén fabricadas en material de aluminio o acero, más concretamente en material de aluminio, ya que este material presenta unas adecuadas características las cuales son totalmente compatibles con el desarrollo de toda actuación

policial, y a su favor hemos de decir que pesa aproximadamente la mitad que el acero. Una defensa extensible de aluminio de 21 pulgadas, puede pesar aproximadamente los 250 gramos, mientras que una defensa de acero con las mismas características puede pesar en torno a los 450 gramos. Desde esta publicación y en base a todo ello, se desaconseja rotundamente la adquisición para la labor policial, ya sea formativa o operativa, de toda defensa extensible que este fabricada con material de polímero en lo que se refiere a sus tramos internos (shafts).

Es cierto que en algunas ocasiones el hecho de realizar la propia apertura con la defensa extensible, le produce un efecto disuasorio al agresor, ya sea por su sonido o por la impresión de verla, pero no debemos de confiar en que siempre sucederá esto puesto que cuando el agresor tiene claras sus intenciones, el hecho de abrir la defensa extensible no suele producir en él ningún tipo de reparo.

Existen algunos modelos de defensas que contienen cordones para facilitar su sujeción, tetones salientes, costuras... desde esta publicación se recomiendan adquirir aquellas defensas extensibles que por el contrario no dispongan de ninguno de estos elementos, ya que los mismos puede darse el caso de que produzcan lesiones no deseadas.

Un modelo estándar de defensa extensible va a estar compuesto al menos por las siguientes piezas:

- Cap, que sería el tapón inicial de la defensa, a través del cual conseguimos cerrar la parte baja de la defensa. En el interior de este cap encontraremos el clip de retención. Este cap ira enroscado al grip.
- Clip de retención, que sería la pieza encargada de retener los shaft cuando estos están recogidos. Este clip marcará el nivel de tensión que adquieren los shaft y dicho nivel de tensión podrá ser aumentado o disminuido en función de la apertura que le demos al clip de retención.
- Junta tórica del cap, que será la encargada de facilitar la unión entre el cap y el grip, e irá alojada al final de la rosca del grip.
- Grip, que sería el chasis de la defensa o lo que viene siendo lo mismo, aquello resultante al desmontar todas las piezas de la defensa. En él se van alojando todas las piezas que componen la defensa extensible.
- Empuñadura, que sería la pieza a través de la cual empuñamos la defensa una vez que procedemos a utilizarla. Existen muchos tipos de empuñaduras en función del modelo de defensa, las más habituales son de vinilo espumado y de goma moldeada. Desde esta publicación aconsejamos la adquisición de aquellas defensas que tiene una empuñadura de goma moldeada, ya que otro tipo de empuñaduras son propensas a ser bastante resbaladizas.
- Shaft medio, es el primer tramo de shaft, el cual una vez extendido queda comprendido entre la parte final del grip y el shaft final.
- Shaft final, es el último tramo de shaft, y este quedaría una vez extendido entre el shaft medio y el tip. Este shaft mientras está cerrado se encuentra en el interior del shaft medio y una vez que lo extendemos sobre sale de la parte final de este,

terminando por quedar frenado gracias a la fricción que se produce con la parte final del shaft medio.

- Tip, sería el tapón final de la defensa extensible, y el mismo es el encargado de recibir la mayor parte del impacto al producir un golpe con esta. El tip se encuentra enroscado a la última parte del shaft final, formando una sola pieza con el shaft medio y el final.

En relación a la longitud de las defensas extensibles podemos observar muchas opciones diferentes en todo el mercado. La elección de la correcta longitud de la misma, vendrá determinada por el tipo de servicio al que se vaya a destinar. No será lo mismo realizar un servicio de paisano donde deberá de primar el porte oculto de la defensa, a realizar un servicio a caballo o de control de masas donde deberá de primar una mayor longitud de la defensa con la que poder garantizarle una correcta seguridad al Policía Local que realice tales funciones.

Los tamaños más habituales de cualquier tipo de defensa son de 16, 21, 26 y 31 pulgadas de longitud extendida. Para servicio normal de seguridad ciudadana, se recomiendan las defensas extensibles de 21 pulgadas, en cambio para paisano normalmente se suelen usar las de 16 pulgadas. En caballería y otros servicios se usarán como mínimo en la mayoría de los casos las de 26 pulgadas.

Las defensas extensibles de 16 pulgadas tendrán aproximadamente 40 centímetros de longitud extendida y 16 centímetros cerradas. Las defensas de 21 pulgadas, tendrán unos 51 centímetros extendidas y 21 centímetros cerradas. Las defensas de 26 pulgadas, tendrán unos 66 centímetros extendidas y 24-25 centímetros cerradas.

El peso de la misma va a variar en función de los materiales con los que se encuentre fabricado cada modelo en concreto. El peso de las defensas extensibles de 21 pulgadas, suelen rondar desde los 250 gramos, hasta los 450-500 gramos.

FUNCIONAMIENTO DE LA DEFENSA EXTENSIBLE

En cuanto al funcionamiento de las defensas extensibles, debemos hacer una clara distinción entre los dos modelos de funcionamiento que podemos optar a la hora de adquirir una defensa extensible. Estos serían por un lado los modelos de fricción y por otro lado los modelos de botón. El uso de las defensas de fricción supone aproximadamente el 90 por ciento de las defensas extensibles que usa la Policía Local. Esto es así por varios motivos, en primer lugar porque son las primeras defensas extensibles que salieron y ello hace que el colectivo policial se encuentre más familiarizado con ellas al venir usándolas desde hace más tiempo. En segundo lugar también repercute el peso, ya que las defensas de botón suelen ser bastante más pesadas. En tercer lugar cobra importancia el aspecto económico, y es que si comparamos varios modelos similares o de la misma marca, veremos que normalmente la de fricción será bastante más económica. En cuarto lugar y desde esta publicación el motivo que más peso tiene para la elección de los modelos de defensas de fricción, viene

determinado por dos razones: simplicidad y efectividad, o lo que viene siendo lo mismo, que sean básicas y operativas. Las defensas de fricción son mucho más simples que las defensas de botón, lo que las convierte en armas con menor probabilidad de que produzcan una avería. Al ser más básicas (no tienen ni la mitad de piezas), hay menos probabilidades de que tengamos problemas con ellas derivados de su funcionamiento. De igual modo y teniendo en cuenta este aspecto, si elegimos las defensas de fricción, tendremos unas armas mas eficaces y operativas de cara al uso policial. También cabe decir que las defensas de botón requieren un mantenimiento mayor a las defensas de fricción, y que por lo tanto si no se le hace dicho mantenimiento estaremos contribuyendo a que puedan averiarse con mayor antelación o continuidad en el tiempo.

Las defensas de fricción se extienden por inercia y se bloquean por fricción (de ahí su nombre), ello es tal que así ya que una vez que extendemos el brazo para producir su apertura, generamos una fuerza mayor a la capacidad de retención producida por el clip de retención. Cuando esto sucede los shaft se liberan de la retención que les estaba produciendo el clip de retención, y estos por la propia inercia de nuestro movimiento producido por el brazo, salen del grip introduciéndose el extremo del shaft final en el extremo del shaft medio, y ambas secciones al ser tronco cónicas terminan firmemente unidas y bloqueadas entre sí. Todo ello será posible cuando produzcamos una apertura correcta de la defensa, si por el contrario no realizamos una correcta apertura, nos encontraremos posiblemente con una interrupción del arma.

Las defensas de botón tienen por el contrario un sistema interno de semi discos, y estos son los causantes del bloqueo en este modelo de defensas. Cuando extendemos el brazo para realizar la apertura de la defensa, esta por inercia se extiende y se termina bloqueando por la acción de estos dos semi discos internos. Para desbloquearla bastará con presionar la base del botón, para que se liberen los semi discos y así podamos cerrarla. También es posible producir una apertura de este modelo de defensa tirando del tip, todo ello gracias al sistema interno que posee.

DIFERENTES TIPOS DE DEFENSAS EXTENSIBLES

Existen diferentes tipos de defensas extensibles en función del cometido con el que las vayamos a utilizar. Obviando la diferenciación que hemos realizado anteriormente con las defensas de fricción y botón en lo que a su sistema interno de apertura y cierre se refiere, aquí vamos a diferenciar los múltiples tipos de defensas extensibles en función del uso al que la vayamos a destinar.

Por un lado tendríamos aquellas defensas de aluminio o acero destinadas al uso policial más usual, comúnmente vistas en operativos de seguridad ciudadana, grupos especiales... Dentro de esta sección y como ya hemos dicho antes, es más común observar las defensas de aluminio para todos estos cometidos, ya que su peso es bastante inferior y las mismas están diseñadas de manera totalmente adecuada para el desarrollo de dichas labores.

Por otro lado tendríamos aquellas defensas destinadas al servicio de paisano, ya que para este tipo de servicio es primordial pasar desapercibidos, y por lo tanto cobra especial importancia la opción del porte oculto. Este tipo de defensas suelen tener modelos de menor tamaño y peso, para facilitar su porte en estos determinados servicios teniendo en cuenta también la comodidad, ya que lo que nos interesa es poder portar en todo momento aquel material que podamos llegar a necesitar, no siendo lo más adecuado dejar el material de trabajo en el vehículo policial para posteriormente cogerlo cuando pensemos que vamos a necesitarlo. Este tipo de defensas suelen tener clips de sujeción para fijarlas en la ropa, con los que de este modo podríamos portarlas sin necesidad de requerir para ello una funda específica.

En el contrario que para el resto de servicios, en lo respectivo a los servicios de paisano, sí que quizás pueda llegar a tener más cabida el uso de las defensas de botón frente a las defensas de fricción, ya que en este tipo de servicios es más probable de que pueda darse el caso en el cual precisemos de realizar una apertura de nuestra defensa haciendo el mínimo ruido posible. Por lo tanto para este tipo de cometidos y desde el punto de vista de esta publicación, sería el único tipo de servicio para el que se recomendarían las defensas extensibles de botón.

Por último, existen ciertos modelos de defensas extensibles diseñadas para usarlas en entornos costeros. Esto es debido a que en estos entornos aumenta la humedad salina, y este es un factor que afecta negativamente al desgaste y consiguiente a la durabilidad de los materiales de la defensa. Es habitual encontrarnos con defensas en las que apreciamos un excesivo desgaste en ciertos materiales, esto en parte puede ser debido a este tipo de entornos costeros. Este tipo de defensas no quiere decir que no vayan a deteriorarse con el paso del tiempo, si no que están fabricadas incluyendo una protección extra para este tipo de entornos, con lo que pueden sobrellevar de una mejor manera la afectación por el salitre.

MANTENIMIENTO DE LA DEFENSA EXTENSIBLE

Todo tipo de defensas extensibles al igual que el resto de armas, requieren de un adecuado mantenimiento cada cierto periodo de tiempo. Todo el mantenimiento que precisa una defensa extensible, es muy básico y con un mínimo de formación se lo podremos hacer nosotros mismos sin la necesidad de precisar de un armero profesional.

El mecanismo de una defensa extensible está diseñado para que funcione de manera seca, por lo que no se precisará de lubricación en ninguno de sus tramos, con lo cual esta deberá de encontrarse en todo momento seca. Al unísono de ello, toda la suciedad que adquieran los tramos, terminará por entrar en la parte interna de la defensa y podrá tanto ocasionar problemas en su apertura, como favorecer a un aumento del desgaste de los componentes. Con lo que la defensa tendrá que encontrarse en todo momento limpia. Por todo ello cuando dicha defensa se moje, se encuentre húmeda o sucia, bastará con desmontarla y limpiar las partes internas de la misma, así como sus tramos

(shaft). Una vez realizada esta limpieza se procederá de nuevo a su montaje, quedando operativa para su nuevo uso.

A diferencia de los modelos de fricción, los cuales no precisan en ningún momento nada de lubricación en sus tramos, en los modelos de botón si es aconsejable lubricar con un poco de aceite sus discos, todo ello para un mejor desarrollo de su función. Esta lubricación nunca ha de hacerse en exceso, de hacerlo así estaríamos contribuyendo a un mal mantenimiento de la misma, lo que podría traernos problemas.

Es importante que comprobemos con cierta frecuencia que el cap se encuentra bien sujeto al grip, de no ser así lo apretaremos con nuestra propia mano (sin necesidad de herramientas) hasta cerciorarnos de que este está correctamente fijado al grip. En este preciso momento procederemos a lubricar con una gota de aceite la junta tórica, enroscando y desenroscando varias veces el cap para cerciorarnos de que el aceite se adhiere a toda la junta de manera correcta.

Del mismo modo que comprobamos que el cap se encuentra correctamente fijado al grip, comprobaremos también que el tip se encuentra fuertemente fijado al shaft final. Si no es así lo apretaremos con contundencia y si con el paso del tiempo observamos que el tip no consiguiera fijarse de manera firme al shaft final, podremos proceder a pegarlo con algún tipo de pegamento fuerte, de modo que nos aseguremos que este quedará fuertemente fijado al tramo final. Hemos de tener en cuenta que en todo momento ha de quedar firme el tip al tramo final, puesto que será con este con el que impactaremos en el objetivo cuando procedamos a golpear con la defensa. Por lo que de no quedar fuertemente sujeto podríamos provocar lesiones no deseadas o perder eficacia en nuestro impacto.

Con el paso del tiempo y en función del uso que le demos a la defensa, es normal que el clip de retención se desgaste, puesto que este es una pieza sujeta a un determinado deterioro. Por ello comprobaremos de igual modo y de manera periódica, que este se encuentra en buen estado y que proporciona la correspondiente sujeción al tramo medio (shaft medio). Es probable que en algún momento observemos que la sujeción de este haya perdido firmeza, por lo que nos encontraríamos que dichos tramos proceden a su apertura o mejor dicho se sueltan de su sujeción con mayor facilidad de la deseada. En este caso deberemos de sacar el clip de retención y proceder a su reparación. Existen herramientas con las que devolver el clip a su forma original, y consigo repararlo. Cuando el clip se cierra más de lo adecuado, es cuando pierde sujeción con respecto al tramo medio, y por ello este tramo se libera con facilidad.

Por ello una vez reparado el clip (para lo que bastará con abrir sus patillas laterales hasta su forma original), procederemos a su montaje y consigo volveremos a disponer de una defensa en óptimas condiciones. De no ser reparable dicho clip de retención, tendremos que adquirir otro nuevo y proceder a su montaje (su coste es muy bajo).

Las empuñaduras también estarán sujetas a desgaste, todo ello producido por el roce de la mano al empuñar la defensa. Una vez que observemos que estas ya están demasiado gastadas o no se encuentran en condiciones óptimas para el trabajo, procederemos a su

sustitución por otra nueva. Para ello simplemente tendremos que rajar con cuidado la empuñadura usada y terminar por quitarla del grip. Una vez extraída, limpiaremos la zona donde se aloja la empuñadura con alcohol, ya que esta zona se encontrará con restos del pegamento antiguo o restos de suciedad acumulada. Una vez limpia la zona, procederemos a colocar las dos tiras de pegamento que deberá de traer la empuñadura nueva, las cuales son unas tiras de papel que traen pegamento en ambas caras, de modo que por una parte las pegaremos al grip y por otra parte pegaremos en ellas la empuñadura nueva, quedando así la defensa de nuevo en óptimas condiciones de uso.

FUNDAS PARA LAS DEFENSAS EXTENSIBLES

Al igual que existen diferentes tipos de defensas, también existen muchos tipos de fundas, como lo son las fundas de polímero, las fundas de plástico, las fundas de cuero, las fundas de cordura... Cada funda tendrá unas características en concreto, pero desde esta publicación se aconsejará la adquisición de aquellas fundas que cumplan una serie de requisitos, los cuales son:

- En primer lugar se recomiendan aquellas fundas que tengan un material de fabricación que sea de calidad y que el mismo soporte caídas, porrazos, tirones, golpes y demás controversias que puedan ocasionarse durante el trabajo policial, todo ello sin perder la sujeción de la defensa ni por supuesto rompiéndose y dejando caer la defensa. Las fundas fabricadas en material de polímero, serán las que cumplirán de un mejor modo con todos los requisitos que vamos a exponer a continuación para ser destinada al servicio policial.
- Dicha funda debe de permitir una rápida extracción de la defensa así como una rápida vuelta a la funda de la misma, o en otras palabras una correcta y rápida transición negativa y positiva de la defensa. Para ello deberá de tener unas adecuadas características que lo permitan.
- Del mismo modo deberán de permitir una introducción de la defensa, ya sea en condición de cerrada o abierta, esto es que se deberá de permitir también que podamos introducir la defensa en medio de una intervención aun no habiendo procedido al cierre de la misma. Al igual que también deberá de permitir la extracción de la defensa cuando esta se encuentre abierta e introducida en la funda, para ello algunas fundas traen una apertura en su lateral que facilita este cometido.
- Es interesante que la funda rote en diferentes posiciones, para así poder ponerla en la posición de porte que nos resulte mas eficaz sin perder comodidad. Al mismo tiempo tendremos que cerciorarnos de que a la vez que rota entre diferentes posiciones, también permita una firme fijación en la postura que deseemos, para que así nos proporcione la suficiente seguridad de que no estará girando en todo momento o con cierta facilidad en los momentos no deseados.
- También es de destacar que el pasador del cinturón se pueda adaptar a los diferentes anchos del cinturón. Existen modelos de cinturones con anchos diferentes,

por lo que es posible que en algunos momentos adquiramos una funda que de no poseer esta característica, no sea válida para determinados cinturones. De este modo podemos adaptar la funda a cualquier tipo de cinturón, sin preocuparnos de que esta misma quede o no bien sujeta por el ancho del cinturón.

- Por último, es muy importante que disponga de un clip de retención que nos permita modificar y adaptar la sujeción de la defensa a la funda, garantizándonos que la defensa no se desprenderá en ningún momento y de manera accidental de la funda. Por otro lado, y gracias a esta característica, nos permitirá elegir el nivel de retención de la defensa en lo que se refiere a su extracción de la funda, pudiendo modificarlo a nuestro antojo en cualquier momento.

Existen modelos de fundas especiales para determinados cometidos, como son el caso de las fundas para uso de paisano o las fundas para servicios especiales (por ejemplo, para los grupos de control de masas, los que suelen llevar fundas acopladas a la pernera del arma). Este tipo de fundas estarán diseñadas para adaptarse de un mejor modo al cometido en concreto para el que estén ideadas.

Por otro lado, también podemos observar las fundas combinadas, que serán las que permitirán el porte de la defensa en conjunción con otra u otras herramientas. En este grupo la más común de ver es la funda de defensa combinada con la funda de esposas. De este modo en un solo elemento (de un tamaño superior a la funda simple) podremos portar la defensa y las esposas.

ACCESORIOS PARA LA DEFENSA EXTENSIBLE

Existen una serie de accesorios para combinar en conjunto con la defensa extensible, estos no podrán ser de un tamaño excesivamente grande, pero a pesar de ello algunos sí que resultan de bastante utilidad. Aquí podemos encontrar los siguientes accesorios:

- Espejos tácticos, los cuales serán acoplables a la defensa, de tal modo que, si por ejemplo tuviéramos que realizar un cuarteo de una esquina o mirar por debajo de un vehículo, bastará con desenfundar la defensa y usar esta herramienta.
- Linternas tácticas, las cuales no precisarán de muchos lúmenes, pero podrán ser de utilidad en ciertos cometidos o mejor dicho cuando nos falle nuestra linterna principal.
- Tapones rompe cristales, con los que podremos proceder a la rotura de algún cristal que precise de rapidez (como por ejemplo las ventanas de un vehículo para poder evacuar un animal que se encuentre al sol en altas temperaturas).
- Tapones personalizados, los cuales llevarán distintas insignias en su base final del cap.
- Tapones sobredimensionados, mediante los cuales podremos mejorar el empuñamiento de la defensa y asegurarnos de un mejor modo que la misma no se nos

escapará con facilidad mientras estemos realizando un ejercicio de entrenamiento o una actuación durante la jornada laboral. Con este mismo tipo de tapón también nos garantizaremos una mejor extracción de la defensa en la funda, ya que mejorará de igual modo el empuñamiento.

Desde esta publicación se recomienda sobre todo el uso de este último tipo de accesorio, el tapón sobredimensionado, ya que gracias a el mejoraremos en gran medida el empuñamiento y la fijación de la defensa a la mano, lo que cobra mucha importancia a la hora de usar la defensa extensible de cara a cualquier tipo de intervención policial.

APERTURA Y CIERRE DE LA DEFENSA EXTENSIBLE

Para conseguir una correcta apertura de la defensa, en primer lugar, tendremos que tener un adecuado empuñamiento. Para ello bastará con sostener de manera firme el grip desde su parte mas baja, dejando aproximadamente una separación de varios dedos con el cap. Mientras más bajo sea empuñe, más fuerza podremos mandar en la apertura. Una vez tengamos un correcto empuñamiento, deberemos de hacer una extensión completa del brazo con la suficiente fuerza para que se liberen ambos tramos. Estos tramos están retenidos por la sujeción del clip de retención, los cuales al realizar una extension fuerte del brazo, se liberarán debido a la propia inercia de nuestro movimiento. Para que esta extensión del brazo sea lo más enérgica posible, es recomendable que se acompañe con un movimiento final de la muñeca, lo que le dará aún más energía.

Una vez que los tramos se han liberado, y siempre que la apertura sea correcta, estos mismos serán bloqueados en su parte final debido a la fuerza centrífuga que hemos ejercido. Los shaft no dejan de ser secciones troncocónicas, las cuales llega un momento en que se agrandan y ellas mismas se bloquean debido a la inercia ejercida. El bloqueo se realizaría en la parte final del shaft medio y en la parte inicial del shaft final.

En relación a la apertura de la defensa, debemos de tener claro hacia donde la haremos, puesto que, si accidentalmente realizamos esta hacia algún objetivo no deseado, podemos provocar serias lesiones. Desde esta publicación se recomienda realizar su apertura hacia arriba siempre que se pueda, ya que de esta manera nos estaremos asegurando en la mayor parte de los casos que no impactaremos con nadie en lo que respecta a su apertura. Del modo que si realizamos una apertura de nuestra defensa hacia la propia amenaza o hacia otra persona de manera accidental, muy probablemente podamos llegar a provocarle serias lesiones por el impacto de la misma. Por lo que en todo momento y salvo casos puntuales donde la técnica de apertura en concreto así lo estime, no se deberá de realizar la apertura de la defensa extensible hacia ninguna persona. Si aplicamos en todo momento e interiorizamos un adecuado método de apertura de la defensa, no deberíamos de tener que preocuparnos por este motivo en ningún momento.

El fallo más común en la apertura de las defensas extensibles, viene determinado por no realizar este de manera totalmente vertical, unido a la ausencia de un adecuado movimiento final de la muñeca.

En las defensas extensibles de botón si se podrá realizar una apertura de la misma con menos fuerza, e incluso tirando levemente con nuestros dedos del tip podremos extender los tramos hasta bloquearlos y fijar así la defensa en condición de abierta.

Para lograr un correcto cierre de la defensa, deberemos de golpear de manera enérgica el tip contra el suelo o una superficie dura. Si por el contrario este golpe lo hacemos en una superficie blanda, difícilmente vamos a conseguir el cierre del mismo. Este movimiento deberá de aplicarse con cierta contundencia, y para que sea lo más enérgico posible se debe de realizar con la defensa de manera totalmente vertical hacia el suelo, siendo lo más aconsejable doblar para ello ambas rodillas (no la cintura), sin tener así la necesidad de tener que mirar en ningún momento la defensa.

Una vez que hemos logrado cerrar los tramos, estos mismos se adentrarán en el interior del grip y serán retenidos por la sujeción del clip de retención. Concretamente el tramo final se introduce dentro del tramo medio y el clip de retención ejerce la sujeción sobre este tramo final. Como dijimos anteriormente, la dureza de esta retención se puede modificar abriendo o cerrando los lados del clip, de modo que mientras más los abramos mayor firmeza nos encontraremos.

El problema más común en lo relacionado con el cierre de las defensas, viene determinado por no realizar este movimiento de manera totalmente vertical hacia el suelo, lo que difícilmente provocará una correcta liberación del bloqueo de ambas secciones troncocónicas.

En relación a la defensa de botón, no podremos bajo ningún concepto golpear el tip contra el suelo o ninguna otra superficie para producir el cierre de la misma, ya que de hacer esto podremos dañar seriamente el mecanismo de la defensa. Para cerrar este tipo de defensas bastará con presionar el botón que contienen en el cap y proceder con nuestra mano a introducir los tramos en el interior de la misma.

LUGAR DE PORTE DE LA DEFENSA EXTENSIBLE

En la actualidad observamos numerosos Policías con diferentes lugares de portes en lo que se refiere a la defensa extensible. Desde esta publicación se anima a que cada Policía pruebe los diferentes lugares de porte que el mismo considere oportunos, y después del entrenamiento y las diferentes pruebas, elija el método que mejor se adapte a sus necesidades de trabajo. No a todos los Policías les tiene por que ir bien una misma condición de porte, y es que cada persona tendrá en primer lugar sus diferentes características personales, y en segundo lugar cada Policía en función de donde trabaje tendrá una serie de cometidos y materiales diferentes al resto. En esta relación de casuísticas podemos hacer a modo de ejemplo, mención a las notables diferencias que puedan tener en su jornada laboral un Policía Local destinado a la seguridad ciudadana

con labores de control del tráfico, a un Policía Local destinado a un grupo de intervención operativa. Lógicamente ninguno de estos dos tendrán las mismas necesidades, ni los mismos medios de dotación, ni el mismo entrenamiento, por lo que puede ser que el lugar de porte de la defensa extensible que le resulte más adecuado a uno de ellos, no le valga en absoluto al otro Policía. También es posible que por la corpulencia física, capacidad física, lesiones, costumbre... y demás diferencias entre varios Policías, hagan que lo que a uno de ellos le sea totalmente válido y operativo, al otro no le resulte eficaz. Por ello decíamos antes que lo mas recomendable es escuchar y formarse en lo referente a la materia, y después probar si eso que te han recomendado es válido para tu jornada laboral, se adapta a tus necesidades y si por lo tanto te resulta efectivo y operativo en tu día a día como Policía Local.

Dicho esto y desde esta publicación vamos a mencionar los dos lugares de porte más extendidos en lo referente a la defensa extensible.

En primer lugar se encontraría el porte justo detrás del arma de fuego (dejando el hueco necesario para no entorpecer una extracción del arma), en modo vertical, con el tip hacia abajo y el cap hacia arriba. Dicho porte resulta cómodo y sobre todo al estar en posición vertical, nos deja más espacio libre en el resto del cinturón para poder alojar otras herramientas policiales. Este quizás sea el porte de la defensa extensible más extendido en la comunidad policial.

En segundo lugar destacamos el porte en la zona delantera del cinturón, justo en la parte final del mismo (cercano a la hebilla del cinturón), de manera horizontal y concretamente en la zona contraria a la mano dominante. Este porte nos quitará algo de más espacio en el cinturón al encontrarse de manera horizontal, pero también tendrá sus ventajas. En primer lugar se aconseja que sea en la zona contraria a la mano dominante para que se facilite la extracción de la defensa con la propia mano dominante desde la funda, ya que de este modo tendrás una mejor zona de acceso y recorrido para la extracción de la defensa. En segundo lugar hacíamos mención a que sea justo cercano a la hebilla para que durante la extracción y teniendo en cuenta la fuerza que haremos para la misma, la funda al estar en contacto con la zona final de alojamiento del cinturón, no pueda pivotar o moverse en el momento de la extracción. Si esto no fuera así y la funda no estuviera bien sujeta, puede darse el caso de que la misma se mueva por la fuerza que haremos durante la extracción de la defensa, y este inconveniente se traduzca en problemas o dificultades a la hora de poder extraer la misma.

El porte delantero y de manera horizontal, facilita una extracción de la defensa extensible así como un enfunde o transición negativa en el uso de la fuerza, de manera mas simple y rápida que el mismo en la zona trasera. El porte en la zona trasera y de manera vertical, no requiere una extracción de la defensa de manera cruzada, lo que también puede influir de manera positiva al darse el caso de que si tuviéramos alguien delante nuestra que nos intentara de impedir la extracción de la defensa, en la zona trasera le resultaría mucho más difícil dificultarnos esta extracción.

Lo que si hemos de tener claro es que la defensa en todo momento y como condición de porte ya sea durante nuestra jornada laboral o durante una formación, habrá de encontrarse en condición de cerrada e introducida en su correspondiente funda. De este modo pasará más desapercibida, nos resultará mucho más fácil extraer la misma, será mucho más cómoda de portar y no permitiremos que la suciedad o las inclemencias del tiempo le afecten de una manera tan perjudicial a la defensa extensible.

MANEJO BÁSICO DE LA DEFENSA EXTENSIBLE

En primer lugar es interesante aclarar que la defensa extensible siempre se extrae de la funda con la mano dominante, sería un error extraerla o incluso portarla con la mano débil y después en el momento de uso cambiarla a la mano dominante.

Para facilitar la extracción de la defensa extensible desde la funda, es recomendable que presionemos la misma en cierto modo contra nuestro cuerpo y no hacia el exterior, ya que así facilitaremos la extracción y por el contrario podemos conseguir que se dificulte la misma.

Desde esta publicación siempre se aconseja realizar un empuñamiento de la defensa algo más bajo del centro de la empuñadura, esto es de tal modo que nuestra mano se coloque entre la mitad de la empuñadura y el cap (cercana al cap). Con este empuñamiento ganaremos control y potencia a la hora de emplear las diferentes técnicas o movimientos con nuestra defensa. La defensa se empuña con la mano al completo, no dejamos ningún dedo o parte interna de la mano sin contacto con la empuñadura, de este modo logramos la suficiente firmeza para que el empuñamiento sea lo más correcto posible.

El enfunde de la defensa en su funda se realiza de manera sencilla, bastará con introducir nuestra defensa con el tip hacia el interior de la funda, quedando de este modo el cap hacia fuera. Si tenemos una adecuada funda, podremos introducir no solo la defensa en condición de cerrada sino que también podremos hacerlo en condición de abierta o extendida.

ZONAS DE IMPACTO CON LA DEFENSA EXTENSIBLE

Hemos de ser conscientes que mediante un impacto con la defensa extensible, podremos provocar lesiones en el agresor. Para ello y siempre que lo hagamos hemos de estar seguros de que la situación lo requiere. Si llegados a ese momento así lo consideramos, hemos de saber que todos los impactos deberán de dirigirse hacia los diferentes centros de masas del agresor. Estos serán aquellas zonas del cuerpo con las que nos puedan poner en riesgo o aquellas que tengan capacidad lesiva hacia nosotros, y que por lo tanto necesitemos de incapacitar. Por ejemplo siempre que alguien nos pretenda herir con algún tipo de arma, tendrá que cogerla con las manos para ello, o siempre que nos pretenda golpear aunque sea sin armas, tendrá que hacerlo o bien con

las manos o con las piernas. Por ello decimos que llegados el momento, precisaremos de incapacitar aquellas zonas del cuerpo que por sus determinadas características pueden ser tendentes a ser usadas contra nuestra integridad física.

A groso modo nos encontraríamos con los brazos y las piernas, donde deberíamos de dirigir los impactos a los músculos mayores de los mismos, estos serán los bíceps y los cuádriceps. Decimos que es totalmente aconsejable dirigir los impactos en estos músculos, puesto que los mismos son los más grandes (de aquellas zonas que probablemente necesitemos incapacitar), y consigo tendremos menos probabilidades de provocar lesiones no deseadas, evitando en todo momento impactar en los huesos. De igual modo estos músculos presentan menos riesgos de lesión que los que podemos encontrar en otro tipo de zonas.

Por todo ello este tipo de técnicas dirigidas al centro de masas de aquellas zonas que pretendemos incapacitar, presentan un alto poder de incapacitación y un bajo poder lesivo frente a otras zonas corporales. Del mismo modo, si estos impactos fallaran en su localización, las zonas cercanas a estas también presentan similares características incapacitantes y lesivas.

Cabe hacer mención a la importancia que tiene impactar en todo momento con la zona más beneficiosa de la defensa. Esto será de tal modo puesto que de esta manera será de la forma con la que podremos enviar mayor nivel de potencia y precisión con la misma. Esta zona será con los últimos 7 centímetros de la misma en su condición de abierta (zona del tip), o con el cap cuando estos impactos sean en la condición de cerrada. Dichos impactos siempre se deberán de realizar de manera perpendicular (aproximadamente con la defensa a unos 45 grados), nunca con la misma de manera vertical y siempre desde arriba hacia abajo, así evitaremos impactos no deseados.

No debemos olvidar que todas nuestras actuaciones han de aplicarse en todo momento respetando la legislación vigente y por lo tanto haciendo cumplir la misma, lo que se apoyará en todo momento desde esta publicación. Eso no quita que pueda haber situaciones en las que necesitemos de generar algún impacto con nuestra defensa extensible hacia un tipo en concreto de agresor, todo ello por su actitud lesiva hacia nosotros o terceras personas, aún sabiendo que este impacto posiblemente le termine causando lesiones. No por ello hemos de pensar que esto quedará fuera de lugar en nuestro ordenamiento jurídico. Vamos a poner un ejemplo, imaginemos una pareja de Policía Local sin apoyos disponibles, la cual está procediendo a denunciar una infracción de tráfico y en el momento de la denuncia el infractor se baja del vehículo por no estar conforme con el mismo. En estos momentos el mismo le recrimina a los agentes el motivo de la denuncia y muestra no estar conforme con ella, pero los agentes le indican que tienen que proceder con la misma. Por ello el infractor, conocido campeón de boxeo a nivel nacional, decide golpear fuertemente al primer Policía Local que se encontraba más cercano a él, dejándolo inconsciente en el suelo. En este momento, conociendo la capacidad lesiva del boxeador y en atención a los hechos ya sucedidos, será totalmente oportuno que el otro Policía Local emplee la defensa extensible contra él, todo ello antes de que dicho boxeador continúe con su intención de agredir a los agentes. Estos hechos

no son inventados, sino que han sido sucedidos en un municipio de Andalucía no hace relativamente mucho tiempo desde la realización de esta publicación.

Con ello en ningún momento y menos desde esta publicación, estamos empujando a emplear la violencia, sino todo lo contrario, pero si llegado el momento hemos de hacerlo en atención a las diferentes casuísticas o necesidades que se nos presenten, no hemos de tener dudas en hacerlo.

BIBLIOGRAFÍA

- “EL ENFRENTAMIENTO POLICIAL ARMADO”, DE DANIEL GARCÍA ALONSO.
- “HECHOS PROVADOS A SANGRE Y FUEGO”, DE ERNESTO PÉREZ VERA.
- “LECCIONES DE SANGRE”, DE CHARLES REMSBERG. QUE APRENDEN LOS POLICÍAS DE SUS ENCUENTROS A VIDA O MUERTE.

TECNOLOGÍAS APLICADAS A LA SEGURIDAD CIUDADANA: VIDEOCÁMARAS, DRONES Y VIGILANCIA INTELIGENTE



AUTOR/ES: SERGIO GONZÁLEZ SÁNCHEZ

TECNOLOGÍAS APLICADAS A LA SEGURIDAD CIUDADANA: VIDEOCÁMARAS, DRONES Y VIGILANCIA INTELIGENTE

Autor: Sergio González Sánchez

EPÍLOGO

En las últimas décadas, hemos asistido a una transformación sin precedentes en el ámbito de la seguridad como consecuencia directa del avance tecnológico. Herramientas que antes eran propias del ámbito militar o industrial, como los sistemas de videovigilancia en red, las aeronaves no tripuladas (drones), los sensores urbanos o la inteligencia artificial aplicada al análisis de datos, han sido progresivamente incorporadas a las labores policiales, redefiniendo la forma en que se detectan, previenen y responden a las amenazas en entornos urbanos y rurales.

Esta evolución tecnológica no solo ha dotado a los cuerpos de seguridad de mayor capacidad operativa, sino que también ha generado nuevos retos jurídicos, éticos y sociales. La aparición de tecnologías de vigilancia masiva, el tratamiento automatizado de datos personales o la utilización de algoritmos de predicción delictiva obligan a repensar los límites entre seguridad y privacidad, y exigen un marco regulatorio claro, proporcional y respetuoso con los principios constitucionales.

Además, en el actual contexto de transformación digital de las Administraciones Públicas, las Policías Locales enfrentan el doble desafío de adaptarse a un entorno tecnológico en rápida evolución, y de hacerlo sin perder de vista su cercanía con el ciudadano, su función preventiva y su papel fundamental en la convivencia social.

En este trabajo se analiza, desde una perspectiva técnica, operativa y jurídica, el papel que desempeñan las tecnologías emergentes en la configuración de una seguridad ciudadana moderna, eficaz y legalmente garantista. Se presta especial atención al uso de videocámaras, drones y sistemas de vigilancia inteligente, así como a los marcos normativos nacionales y europeos que regulan su aplicación. También se abordan los límites éticos que deben respetarse en su implementación para avanzar hacia una seguridad ciudadana tecnológicamente avanzada, pero siempre compatible con los derechos fundamentales, la transparencia institucional y la confianza de la ciudadanía.

ÍNDICE

1. VIDEOVIGILANCIA EN ENTORNOS URBANOS
 - 1.1. Evolución tecnológica
 - 1.2. Funciones de las videocámaras
 - 1.3. Marco legal
 - 1.4. Buenas prácticas en videovigilancia

- 1.5. Retos actuales y futuros
2. DRONES EN LA ACTUACIÓN POLICIAL
 - 2.1. Tipologías de drones utilizados
 - 2.2. Aplicaciones prácticas
 - 2.3. Requisitos normativos
 - 2.4. Limitaciones, desafíos y riesgos
3. VIGILANCIA INTELIGENTE Y ANALÍTICA DE DATOS
 - 3.1. Inteligencia artificial aplicada a la seguridad
 - 3.2. Ejemplos de vigilancia inteligente
 - 3.3. Riesgos legales y éticos
 - 3.4. Normativa aplicable
4. CONSIDERACIONES JURÍDICAS Y CONSTITUCIONALES
 - 4.1. Derecho a la intimidad personal y familiar (art. 18.1 CE)
 - 4.2. Derecho fundamental a la protección de datos personales (art. 18.4 CE)
 - 4.3. Principios de legalidad, necesidad, proporcionalidad y control
 - 4.4. Transparencia, información y derechos del ciudadano
5. FUTURO DE LA TECNOLOGÍA POLICIAL
 - 5.1. Cámaras corporales (bodycams)
 - 5.2. Sensores urbanos conectados (Internet of Things - IoT)
 - 5.3. Robots y sistemas autónomos
 - 5.4. Plataformas de mando integradas
6. CONCLUSIÓN
7. BIBLIOGRAFÍA

1. VIDEOVIGILANCIA EN ENTORNOS URBANOS

La videovigilancia se ha consolidado como una de las herramientas tecnológicas más extendidas en la gestión de la seguridad ciudadana. Su presencia en espacios públicos, edificios oficiales, centros de transporte o zonas de especial protección no solo cumple una función preventiva y disuasoria, sino que también permite apoyar de forma decisiva la labor policial operativa y judicial. Sin embargo, su uso debe estar firmemente

regulado, dada la afectación que puede tener sobre derechos fundamentales como la intimidad, la protección de datos o la libertad de circulación.

1.1. Evolución tecnológica

La primera cámara de vigilancia fue creada durante la Segunda Guerra Mundial y desarrollada por Walter Bruch. Su propósito inicial era monitorear el lanzamiento de los cohetes V2. No obstante, aunque estas cámaras surgieron con la idea de vigilar, no empezaron a emplearse para fines de seguridad hasta el año 1969.

La implantación de sistemas de videovigilancia en entornos urbanos comenzó tímidamente a finales del siglo XX, con cámaras analógicas de baja resolución, sistemas cerrados de televisión (CCTV) y grabación local en soporte físico. Estos sistemas requerían supervisión manual y apenas permitían un control en tiempo real.

Con la llegada del video IP (Protocolo de Internet), los sistemas evolucionaron hacia redes digitales. La videovigilancia IP es una tecnología de monitoreo visual que combina las prestaciones analógicas de los sistemas tradicionales de CCTV (Circuito Cerrado de Televisión) con las ventajas digitales de las redes IP (Protocolo de Internet). Esta integración permite controlar imágenes y sonido tanto de forma local como remota, además de procesar digitalmente el video para funciones como el reconocimiento de matrículas o de rostros, entre otras aplicaciones.

Su instalación suele ser más práctica y económica que la de un CCTV convencional, ya que utiliza la red de datos de la empresa, es decir, el mismo cableado destinado a Internet, correo electrónico y otros servicios de comunicación, evitando así la necesidad de tender cables coaxiales exclusivos para el sistema de videovigilancia. Debido a su flexibilidad y funcionalidad, la mayoría de los sistemas actuales están dejando atrás la tecnología analógica y adoptando soluciones IP, aprovechando mejor la infraestructura de red ya existente.

Entre los avances recientes más relevantes se encuentran la posibilidad de conexión inalámbrica

—que incluso elimina la necesidad de cableado físico—, la alta calidad de imagen que proporcionan las cámaras megapíxel, y la incorporación de sistemas inteligentes para procesar video, gestionar eventos o contabilizar datos. También es posible grabar vídeo a baja frecuencia de fotogramas o activar la grabación únicamente cuando se detecta movimiento en áreas específicas o en horarios determinados.

En definitiva, podemos decir que el video IP ha permitido:

- La transmisión de vídeo en alta definición en tiempo real.
- El acceso remoto desde centros de control o dispositivos móviles.
- El almacenamiento automatizado en servidores o en la nube.
- La integración con software de analítica de vídeo, incluyendo reconocimiento facial, detección de movimiento, objetos abandonados o multitudes.

En los últimos años, la integración de inteligencia artificial y machine learning ha abierto nuevas posibilidades, como la detección predictiva de comportamientos anómalos, la clasificación automatizada de incidentes o la generación de alertas automáticas sin necesidad de supervisión constante.

1.2. Funciones de las videocámaras

Las funciones de la videovigilancia en el ámbito urbano pueden agruparse en varios niveles de actuación:

- **Prevención del delito:** Su sola presencia genera un efecto disuasorio frente a comportamientos ilícitos, actos vandálicos o agresiones.
- **Intervención inmediata:** Permiten a los operadores de los centros de control detectar situaciones en curso (peleas, robos, altercados, accidentes) y coordinar la respuesta policial en tiempo real, reduciendo los tiempos de reacción.
- **Obtención de pruebas:** Las grabaciones pueden servir como prueba en procedimientos penales o administrativos, siempre que se cumplan los requisitos legales de integridad, custodia y autorización.
- **Control de tráfico y movilidad:** Las cámaras fijas o móviles ayudan a gestionar la circulación, detectar infracciones, controlar accesos restringidos y planificar medidas de movilidad urbana.
- **Protección de infraestructuras críticas y eventos multitudinarios:** Como conciertos, manifestaciones, fiestas locales o grandes celebraciones deportivas.

Además, la videovigilancia urbana puede integrarse con otras tecnologías como sensores acústicos, sistemas de lectura automática de matrículas (LPR), cámaras térmicas o sistemas de megafonía.

1.3. Marco legal

El uso de videocámaras por las Fuerzas y Cuerpos de Seguridad en espacios públicos está regulado por un marco legal específico y garantista, que busca equilibrar la eficacia policial con la protección de derechos fundamentales.

Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Establece en su artículo 6 los principios de utilización de las videocámaras siendo estos los siguientes:

- **Proporcionalidad:** El uso de las cámaras siempre debe responder a una necesidad real y concreta, aplicando dos criterios:
 - **Idoneidad:** Solo se pueden utilizar si son realmente adecuadas para garantizar la seguridad ciudadana en una situación específica.

- Intervención mínima: Se debe valorar si la finalidad que se busca justifica la posible afectación a derechos fundamentales como el honor, la intimidad o la propia imagen de las personas.

- Riesgo o peligro: Las cámaras fijas solo pueden instalarse si existe un riesgo razonable para la seguridad ciudadana, mientras que las cámaras móviles solo pueden usarse si hay un peligro concreto.

Conforme al artículo 4 para la autorización de videocámaras, según el principio de proporcionalidad, solo se pueden instalar cuando sea realmente necesario para:

- Proteger edificios e instalaciones públicas, así como sus accesos.
- Vigilar instalaciones estratégicas importantes para la defensa nacional.
- Detectar o probar infracciones que afecten a la seguridad ciudadana.
- Prevenir daños a personas o bienes.

Las autorizaciones para la instalación de cámaras fijas de videovigilancia se recogen en el artículo 3 de dicha ley, indicando que cuando las Fuerzas y Cuerpos de Seguridad del Estado o las policías locales quieren instalar cámaras fijas, la autorización la otorga el Delegado del Gobierno de la Comunidad Autónoma correspondiente. Previamente, debe emitirse un informe de una Comisión presidida por el Presidente del Tribunal Superior de Justicia de esa Comunidad.

Si la Comisión considera que la instalación de cámaras fijas vulnera los principios establecidos en el artículo 4 de la Ley (como proporcionalidad, idoneidad o respeto a la intimidad), no podrá autorizarse.

La resolución que autoriza la instalación debe ser detallada y explicar:

- El lugar exacto que se va a vigilar.
- Las condiciones o limitaciones de uso, por ejemplo: prohibición de grabar sonido salvo que exista un riesgo concreto.
- Requisitos para las personas que gestionarán las imágenes y sonidos.
- Las medidas que garanticen el respeto de las leyes vigentes.
- Las características técnicas de las cámaras, el área que pueden grabar y la duración de la autorización, que no puede superar un año (después habrá que renovarla).

En todo caso, la autorización puede ser revocada si cambian las circunstancias o se incumplen los requisitos.

No está permitido grabar el interior de viviendas, vestíbulos u otros lugares especialmente protegidos, excepto si hay consentimiento del titular o autorización judicial.

Tampoco se pueden grabar conversaciones privadas. Si se captan por accidente imágenes o sonidos prohibidos, deben destruirse de inmediato.

Con respecto a la autorización de videocámaras móviles se recoge en el artículo 5 que en los lugares públicos donde ya haya cámaras fijas autorizadas, también se pueden emplear cámaras móviles. Sin embargo, para grabar imagen y sonido de forma conjunta, debe existir un peligro concreto y cumplirse los requisitos que establece la ley (especialmente los del artículo 6).

Además, las videocámaras móviles se pueden utilizar en otros espacios públicos distintos a los que tienen cámaras fijas.

La autorización corresponde al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad.

La resolución que aprueba el uso de estas cámaras debe comunicarse a la Comisión de Videovigilancia (mencionada en el artículo 3) en un plazo máximo de 72 horas.

En casos de urgencia extrema donde no es posible obtener autorización a tiempo, se pueden usar videocámaras móviles para grabar imágenes y sonidos. En estos casos, se debe informar igualmente, en un máximo de 72 horas, tanto al máximo responsable provincial como a la Comisión.

Si la Comisión de Videovigilancia emite un informe negativo, la grabación obtenida debe ser destruida inmediatamente por la autoridad que la custodia.

Si la grabación captara la comisión de hechos que pudieran ser constitutivos de ilícitos penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad a disposición judicial con la mayor inmediatez posible, en el plazo máximo de setenta y dos horas.

En cuanto a la instalación de videocámaras o de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico, se recoge en la disposición adicional octava y se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, y demás normativa específica en la materia, y con sujeción a lo dispuesto en las Leyes Orgánicas 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, en el marco de los principios de utilización de las mismas previstos en esta Ley.

Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

En los artículos 3 y 6 reconoce la competencia de los alcaldes o el concejal competente en materia de seguridad ciudadana, respecto a la policía local de su municipio para la

formulación de la solicitud para las instalaciones fijas y móviles de videocámaras. Esta solicitud se dirigirá al Delegado de Gobierno en la Comunidad Autónoma.

En el artículo 17 establece que los órganos facultados para formular las solicitudes de instalaciones fijas de videocámaras o de utilización de videocámaras móviles, conforme a los artículos anteriormente mencionados, son los que deben custodiar las grabaciones obtenidas, y encargarse de su posterior destino, incluyendo la inutilización o destrucción.

La destrucción según el artículo 18 de las imágenes se realizará por cualquier modalidad que permita el borrado o inutilización de las grabaciones, en el plazo máximo de un mes desde el día de su captación, excepto en el caso que aparezcan infracciones penales o administrativas graves o muy graves en materia de seguridad pública.

Por otra parte, el Real Decreto recoge en su capítulo V que abarca de los artículos 21 al 25 los derechos de los ciudadanos que incluyen los siguientes:

- Información al público: la información al público de la existencia de instalaciones fijas de videocámaras es responsabilidad de la autoridad que ha otorgado la autorización y se realizará con una placa informativa donde figurará el pictograma de una cámara de vídeo y un panel complementario informativo con una descripción genérica de la zona de vigilancia y las autoridades responsables de la autorización y custodia de las grabaciones sin especificar el emplazamiento concreto de las videocámaras.
- Derecho de acceso a las grabaciones: Las personas que consideren que figuran en grabaciones realizadas con videocámaras, podrán ejercer el derecho de acceso a las mismas, mediante solicitud a la autoridad encargada de las mismas.
- Derecho a la cancelación de grabaciones: Si como consecuencia del ejercicio del derecho de acceso a la grabación el interesado considera que las imágenes y sonidos no se ajustan a la Ley Orgánica 4/1997, podrá solicitar a la autoridad de custodia la cancelación de las mismas o esta acordarla de oficio.

Por último, en la disposición adicional única se regula el régimen aplicable a las videocámaras para la vigilancia, control y disciplina del tráfico.

En esta disposición se establece que las cámaras usadas para vigilar, controlar y sancionar el tráfico en vías públicas se regulan por lo que indica la disposición adicional octava de la Ley Orgánica 4/1997 y por esta disposición adicional.

La instalación y uso de estas cámaras debe ser autorizada por las Administraciones públicas que tengan competencias en materia de tráfico.

La resolución que permite instalar y usar cámaras fijas debe detallar:

- Las calles o tramos de vías que pueden ser grabados.
- Las medidas para proteger la confidencialidad, integridad y disponibilidad de las grabaciones.

- El órgano responsable de custodiar esas imágenes y resolver las peticiones de acceso o eliminación de datos.

Esta autorización no tiene plazo de caducidad, siempre que no cambien las circunstancias que la justificaron.

En el caso del Estado, la decisión corresponde al Director General de Tráfico.

Las cámaras móviles que se usen para controlar el tráfico no necesitan esta autorización formal, pero su uso debe seguir los mismos principios de protección y conservación de los datos.

La gestión de las grabaciones (custodia, conservación y peticiones de acceso o cancelación) corresponde a los órganos que designen las Administraciones competentes.

En la Administración General del Estado, esta tarea la asume el responsable de los servicios provinciales de la Jefatura Central de Tráfico.

Si estas cámaras se utilizan junto con dispositivos que miden datos como la velocidad de los vehículos, estos aparatos deben cumplir las normas metrológicas correspondientes.

Si las Fuerzas y Cuerpos de Seguridad usan estas cámaras para objetivos diferentes al control del tráfico, deberán hacerlo conforme a la Ley Orgánica 4/1997 y el Reglamento.

Si el uso es por parte de Unidades de Policía Judicial, se aplicará además lo previsto en la Ley de Enjuiciamiento Criminal y su normativa específica.

Protección de datos personales

Por último, toda grabación de imágenes que permita identificar a personas se considera un dato personal y, por tanto, debe respetar:

- Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Aplicable a toda la Unión Europea.
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
- La Ley Orgánica 3/2018, de Protección de Datos y garantía de los derechos digitales (LOPDGDD), que adapta el RGPD al ordenamiento jurídico español.
- Las resoluciones y directrices de la Agencia Española de Protección de Datos (AEPD).

1.4. Buenas prácticas en videovigilancia

El uso responsable y eficaz de la videovigilancia requiere una correcta planificación, gestión y control. Algunas recomendaciones y estándares de buena práctica incluyen:

- Informar a la ciudadanía mediante carteles visibles, con pictogramas y referencias al responsable del tratamiento.
- Establecer políticas internas claras sobre uso, acceso y custodia de las grabaciones.
- Limitar el acceso a las imágenes al personal autorizado y mantener un registro de accesos para garantizar la trazabilidad.
- Conservar las imágenes solo durante el tiempo legalmente previsto (normalmente 30 días), salvo que se vinculen a una investigación o procedimiento.
- No utilizar cámaras con funciones de zoom intrusivo o grabación de sonido, salvo autorización expresa y justificada.
- Realizar evaluaciones de impacto en privacidad, especialmente si se combinan tecnologías sensibles como IA o reconocimiento facial.

1.5. Retos actuales y futuros

El despliegue masivo de sistemas de videovigilancia plantea retos clave para los próximos años:

- Asegurar su compatibilidad con las libertades civiles.
- Evitar la vigilancia masiva indiscriminada.
- Fortalecer los mecanismos de control externo (judicial, institucional y ciudadano).
- Formar a los operadores y mandos policiales en ética del uso de la tecnología.
- Evaluar permanentemente la eficacia real del sistema y su aceptación social.

2. DRONES EN LA ACTUACIÓN POLICIAL

El uso de sistemas aéreos no tripulados (UAS), comúnmente denominados drones, ha supuesto una revolución operativa para las Fuerzas y Cuerpos de Seguridad, especialmente en lo que respecta a tareas de vigilancia, observación, apoyo en emergencias y gestión de eventos multitudinarios. Su capacidad para cubrir grandes áreas, acceder a zonas inaccesibles por tierra, operar en tiempo real y ofrecer una perspectiva aérea precisa los convierte en una herramienta altamente eficaz.

Sin embargo, el despliegue de drones por parte de policías locales requiere el cumplimiento de estrictas normativas aeronáuticas y de protección de datos, así como una formación técnica y operativa rigurosa de los agentes implicados.

2.1. Tipologías de drones utilizados

Existen diversas clases de drones utilizados en el ámbito policial, cuya elección depende del tipo de misión, del entorno y de la duración de vuelo necesaria.

- **Multirrotores:** Son los más utilizados en entornos urbanos. Tienen la capacidad para ingresar a zonas accesibles, despegue y aterrizaje vertical y sencillo, se pueden mantener con vuelo suspendido y tienen precios más económicos. Son ideales para vigilancia estática, control de tráfico o intervención rápida. Por contra tiene el vuelo limitado, son ruidosos y no pueden volar con viento o lluvia fuerte.
- **Drones de ala fija:** Su estructura les permite vuelos de largo alcance con menor consumo energético, son silenciosos, pueden volar a gran altura, son más aerodinámicos y pueden volar durante más tiempo. Sin embargo, necesitan una zona plana para aterrizar y despegar, ocasionalmente pueden necesitar un riel lanzador, el despegue tiene que ser asistido por una persona manualmente, tienen dificultad para entrar en lugares cerrados, son más costosos y menos compactos. Son adecuados para la vigilancia perimetral de zonas rurales, agrícolas o forestales, y para operaciones de seguimiento en espacios abiertos.
- **Drones con cámara térmica o visión nocturna:** Resultan fundamentales en operaciones nocturnas, rescates en baja visibilidad, búsqueda de personas desaparecidas, detección de incendios o vigilancia discreta.
- **Drones híbridos:** Los drones híbridos son aeronaves no tripuladas creadas para aprovechar lo mejor de dos mundos: la gran autonomía y capacidad de cobertura de los drones de ala fija, junto con la agilidad y facilidad de maniobra de los multirrotores. Gracias a su diseño especial, pueden cambiar entre el vuelo horizontal, que les permite recorrer largas distancias, y el despegue y aterrizaje vertical. Esto los convierte en una opción muy versátil para operar tanto en entornos urbanos como en amplias zonas rurales. Aunque más complejos y costosos, ofrecen gran versatilidad.

2.2. Aplicaciones prácticas

Los drones tienen un uso cada vez más extendido en funciones policiales, tanto preventivas como reactivas. Algunas de sus aplicaciones más frecuentes son:

- **Vigilancia en concentraciones multitudinarias:** Permiten monitorizar grandes aglomeraciones gracias a sus cámaras de alta definición y sensores, detectando cualquier altercado, accidente o incidencia que requiera intervención. Esto facilita enviar recursos de forma más eficaz y tomar decisiones más precisas gracias a la transmisión de vídeo en tiempo real.
- **Control y disciplina del tráfico:** Se utilizan para supervisar la circulación y reforzar la seguridad vial.
- **Servicio en playas:** Colaboran con socorristas y otros dispositivos desplegados, mejorando la capacidad de respuesta ante emergencias.

- Investigación y análisis en catástrofes: Ofrecen una vista aérea de zonas de difícil acceso tras incendios, inundaciones u otros desastres naturales. Ayudan a mapear áreas dañadas, generar panorámicas 360° o vídeos geo-referenciados para valorar la magnitud de los daños.
- Actuación en siniestros viarios e incendios: Facilitan inspecciones oculares y el análisis de escenarios como accidentes de tráfico o incendios en edificios e industrias, con el mínimo impacto sobre el lugar.
- Búsqueda y rescate: Equipados con cámaras térmicas y de gran alcance, proporcionan información detallada de la zona de búsqueda. También pueden transportar y dejar caer objetos de auxilio a personas en peligro.
- Protección de autoridades y comitivas: Acompañan al dispositivo policial desde el aire, ofreciendo una visión más completa del entorno y del recorrido.
- Prevención de riesgos con mercancías peligrosas: Permiten reconocer y medir el alcance de un vertido o accidente sin exponer al personal, aumentando la seguridad del operativo.
- Supervisión de otros drones: Ayudan a controlar el uso de drones dentro del municipio, en cumplimiento de las ordenanzas locales que regulan zonas de vuelo restringidas y seguras, protegiendo la intimidad y la seguridad de espacios públicos.
- Vigilancia medioambiental: Sirven para controlar áreas naturales, prevenir incendios forestales o detectar vertidos contaminantes.
- Apoyo en persecuciones y seguimiento de vehículos: Brindan visión aérea en tiempo real para coordinar a las patrullas en tierra sin necesidad de intervención directa inmediata.

2.3. Requisitos normativos

El uso de drones en España está regulado por la normativa europea común y por legislación nacional complementaria. Las operaciones por parte de Fuerzas y Cuerpos de Seguridad deben ajustarse a la normativa aeronáutica que en España se rige por un sistema dual que combina normativa europea con normativa nacional, siendo estas las siguientes:

- Reglamento de Ejecución (UE) 2019/947 de la Comisión, de 24 de mayo de 2019, relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas. establece las categorías de operación (abierta, específica y certificada), así como los requisitos para operadores y pilotos.
- Reglamento Delegado (UE) 2019/945 de la Comisión, de 12 de marzo de 2019, sobre los sistemas de aeronaves no tripuladas y los operadores de terceros países de sistemas de aeronaves no tripuladas.
- Real Decreto 517/2024, de 4 de junio, por el que se desarrolla el régimen jurídico para la utilización civil de sistemas de aeronaves no tripuladas (UAS), y se modifican

diversas normas reglamentarias en materia de control a la importación de determinados productos respecto a las normas aplicables en materia de seguridad de los productos; demostraciones aéreas civiles; lucha contra incendios y búsqueda y salvamento y requisitos en materia de aeronavegabilidad y licencias para otras actividades aeronáuticas; matriculación de aeronaves civiles; compatibilidad electromagnética de los equipos eléctricos y electrónicos; Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea; y notificación de sucesos de la aviación civil.

Además, cuando el dron incorpore sistemas de captación de imágenes o sonido, se aplican los principios del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2.4. Limitaciones, desafíos y riesgos

A pesar de su enorme potencial, la incorporación de drones en la actividad policial enfrenta ciertas limitaciones técnicas, normativas y operativas:

- Condiciones meteorológicas: La lluvia, el viento fuerte o la baja visibilidad pueden impedir su uso seguro. En zonas costeras o montañosas, esto puede limitar su utilidad.
- Restricciones al vuelo: No se puede operar libremente en todos los espacios. Existen zonas restringidas como áreas próximas a aeropuertos, instalaciones estratégicas, centrales nucleares o eventos protegidos. Se requiere autorización especial en algunos casos.
- Costes operativos: La adquisición de equipos, el mantenimiento, las baterías, el software de gestión y la formación técnica suponen un desembolso importante para las administraciones locales.
- Riesgos legales y éticos: El mal uso de drones puede suponer una intromisión ilegítima en la vida privada, especialmente en el caso de grabaciones sin base legal. También es necesario extremar el cuidado en operaciones en viviendas, patios interiores o espacios privados.
- Aceptación social: La percepción de la ciudadanía sobre el uso de drones varía. Es fundamental mantener una política de transparencia, comunicación institucional y formación ética del personal.

Entre los riesgos del manejo de los drones podemos encontrar:

- Caídas desde diferentes alturas.
- Golpes o impactos, así como la caída de objetos o materiales.

- Cortes provocados por el contacto con las hélices, tanto mientras están girando como durante las operaciones de transporte.
- Posibles incendios o explosiones ocasionados por las baterías de litio que alimentan el dron y su control remoto.
- Riesgos de contactos eléctricos o térmicos.
- Riesgos químicos derivados del contacto con las baterías de litio que utilizan estas aeronaves.
- Sobreesfuerzos y posturas incómodas por la posición que debe mantener el piloto durante el vuelo.
- Sobreesfuerzos y posturas inadecuadas al cargar y trasladar manualmente el equipo.
- Estrés térmico.
- Fatiga visual debido al uso continuado de pantallas o gafas FPV.
- Sobrecarga mental por la atención constante que exige el pilotaje.

Para hacer frente a estos riesgos es importante que durante el tiempo de vuelo, tanto los pilotos como los observadores deben encontrarse en perfectas condiciones, no pudiendo operar con cuadros de estrés y fatiga, ni con merma de cualquier condición psicofísica que afecte al vuelo seguro.

Es aconsejable que los pilotos y sus auxiliares lleven un casco protector de emergencias para evitar accidentes en caso de caída del dron, así como guantes y gafas protectoras a la hora de manipular la aeronave, asegurándose siempre que la fuente de energía este desconectada, evitando que las hélices y rotores se pongan en marcha.

Igualmente, no hay que olvidar que no se debe de volar en condiciones climatológicas adversas como en el caso de viento, calima, niebla, tormenta solar, lluvia fuerte o nevada. Y que hay que tener cuidado con las baterías de litio que utiliza el dron ya que puede incendiarse o explotar, por lo que hay que evitar guardarla en sitios donde la humedad o el calor pueda llegar a valores extremos.

Permanecer durante mucho tiempo en una misma posición, ya sea sentado o de pie, puede llevarnos a adoptar posturas incómodas o forzadas para mantener el control del dron. Por eso, es recomendable hacer ejercicios de estiramiento antes y después de cada sesión de vuelo. También es importante cambiar con frecuencia la posición de los pies, prestar atención a los movimientos del cuello y evitar mantenerlo en hiperextensión de forma continuada.

El uso repetido del mando puede provocar lesiones articulares en los dedos debido a los movimientos constantes. Para prevenirlo, conviene planificar pausas que permitan relajar y recuperar la musculatura de las manos; además, estas pausas contribuyen a reducir la sobrecarga mental que supone el pilotaje.

Tampoco debemos olvidar los riesgos relacionados con las PVD (pantallas de visualización de datos). Tener la pantalla muy cerca de los ojos obliga a un esfuerzo visual constante para mantener el enfoque, algo que se intensifica si utilizamos gafas FPV (que muestran imágenes en primera persona), ya que el cerebro debe procesar al mismo tiempo dos imágenes distintas. Es importante parpadear con frecuencia para mantener la córnea hidratada y, siempre que el servicio lo permita, hacer pausas breves de unos cinco minutos, que además ayudan a aliviar la carga cognitiva que implica esta actividad tan exigente.

Algunos especialistas en prevención aconsejan usar lágrimas artificiales o lentes de contacto con alta permeabilidad y elevado contenido de agua. Sin embargo, es preferible no emplearlas sin la recomendación expresa de los servicios médicos de prevención o del oftalmólogo de confianza.

3. VIGILANCIA INTELIGENTE Y ANALÍTICA DE DATOS

La incorporación de la inteligencia artificial (IA) y el análisis masivo de datos (Big Data) en los sistemas de vigilancia pública ha inaugurado una nueva etapa en la forma en que se concibe la prevención, detección y reacción ante situaciones de riesgo. La denominada “vigilancia inteligente” permite automatizar procesos que antes dependían de la supervisión humana continua y ampliar exponencialmente la capacidad operativa de las Fuerzas y Cuerpos de Seguridad.

Este cambio tecnológico, sin embargo, plantea desafíos considerables en términos de legalidad, ética, transparencia y proporcionalidad, dado que muchos de estos sistemas procesan datos personales de forma automatizada, incluso sin intervención directa de la persona afectada.

3.1. Inteligencia artificial aplicada a la seguridad

La IA en seguridad ciudadana se basa en algoritmos capaces de aprender y tomar decisiones a partir de grandes volúmenes de datos recogidos por sensores, cámaras, redes sociales, registros policiales u otras fuentes. A través de estos algoritmos es posible:

- Detectar patrones de comportamiento anómalos, como aglomeraciones inusuales, movimientos contrarios al flujo normal o presencia prolongada en lugares sensibles.
- Predecir zonas o franjas temporales de riesgo delictivo mediante análisis estadístico avanzado.
- Cruzar información en tiempo real entre bases de datos policiales, registros de vehículos y sistemas de identificación.
- Generar alertas automáticas ante comportamientos que se salen del rango habitual (como objetos abandonados o gestos agresivos).

- Asignar recursos policiales de forma más eficiente según datos históricos y proyecciones futuras.

La ventaja de estos sistemas radica en su capacidad de escalabilidad y respuesta rápida, pero su aplicación debe estar sujeta a control humano, supervisión legal y responsabilidad institucional.

3.2. Ejemplos de vigilancia inteligente

Algunos de los usos más destacados de vigilancia inteligente en contextos policiales incluyen:

- Reconocimiento facial en tiempo real: Permite identificar personas buscadas, desaparecidas o con órdenes judiciales vigentes. Su uso debe ser puntual, justificado y proporcional, con una base legal específica. Actualmente está sujeto a fuertes restricciones en la UE por su potencial impacto sobre derechos fundamentales, como el derecho a la intimidad y la libertad de circulación.
- Lectura automática de matrículas (LPR/ANPR): Las cámaras dotadas de este sistema identifican vehículos por su matrícula y la comparan con bases de datos policiales. Se utiliza para detectar vehículos robados, controlar accesos en zonas de tráfico restringido, localizar infractores reincidentes y generar alertas ante vehículos sospechosos.
- Análisis predictivo del crimen: Mediante el procesamiento de datos históricos, sociales y criminales, los algoritmos pueden predecir con cierta fiabilidad dónde es más probable que ocurra un delito. Esto permite a la policía anticiparse con presencia preventiva. Sin embargo, no debe sustituir nunca el juicio humano, ya que puede consolidar sesgos o discriminaciones históricas.

3.3. Riesgos legales y éticos

El uso de estas tecnologías debe equilibrar la mejora en seguridad con la protección de los derechos y libertades fundamentales. Entre los riesgos más importantes se encuentran:

- Discriminación algorítmica: Los algoritmos pueden amplificar sesgos si se entrenan con datos históricos no equilibrados. Por ejemplo, si los datos están concentrados en ciertas zonas con población vulnerable, el sistema puede considerar que siempre hay más delitos en esos barrios, perpetuando la sobrevigilancia.
- Pérdida de anonimato en espacios públicos: La vigilancia automatizada mediante cámaras con reconocimiento facial o comportamiento puede convertir en “sospechoso” a cualquier ciudadano, simplemente por pasar por determinadas zonas, afectando al derecho a circular libremente sin ser identificado.
- Tratamiento masivo y opaco de datos personales: Muchos sistemas funcionan con algoritmos de empresas privadas, sin transparencia sobre su funcionamiento. Además, está el fenómeno conocido como «caja negra», que se produce cuando el

proceso interno del sistema resulta tan complejo que las personas no pueden entender cómo funciona realmente. Esto puede provocar que se acepten como correctos resultados que, en realidad, podrían ser incorrectos o injustos.

- Evaluación de impacto y garantías legales: Es necesario realizar evaluaciones de Impacto en Protección de Datos cuando se implementan tecnologías que puedan suponer alto riesgo, como el uso generalizado de IA, vigilancia biométrica o decisiones automatizadas sin intervención humana. Además, exige el respeto al principio de minimización: solo deben tratarse los datos estrictamente necesarios para la finalidad legítima perseguida.

3.4. Normativa aplicable

El marco jurídico que regula la vigilancia inteligente en España y la Unión Europea se basa en las siguientes normas:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Este reglamento se aplica según el artículo 2 a todo tratamiento automatizado de datos personales, reconociendo en su artículo 22 que todo interesado tendrá derecho a no ser objeto de decisiones exclusivamente automatizadas.

- Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales: Esta ley complementa el RGPD en España.
- Directrices del Comité Europeo de Protección de Datos (CEPD) y del Supervisor Europeo de Protección de Datos (SEPD).
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales: Esta ley se aplica a tratamientos realizados por autoridades públicas con fines de prevención e investigación de delitos.
- Por último, hay que hacer referencia al Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se aprueba el conocido como Reglamento de Inteligencia Artificial. Este pionero reglamento no se aplicará cuando la Inteligencia Artificial se utilice con fines militares, de defensa o de seguridad nacional, y regula los sistemas empleados por la IA para limitar los peligros de esta tecnología sin perjudicar la innovación. En su artículo 5.1.h) autoriza el uso de tecnologías de reconocimiento facial en casos de emergencia como podría ser una amenaza terrorista, identificar a un sospechoso o localizar un menor desaparecido.

4. CONSIDERACIONES JURÍDICAS Y CONSTITUCIONALES

El uso de tecnologías aplicadas a la seguridad ciudadana, como videocámaras, drones, sensores y algoritmos de vigilancia inteligente, debe enmarcarse en un sistema jurídico que garantice la compatibilidad entre la eficacia policial y el respeto pleno a los derechos fundamentales reconocidos en la Constitución Española y en el Derecho de la Unión Europea. La regulación no solo es necesaria, sino que constituye una garantía para la legitimidad de la actuación policial y para la confianza ciudadana en las instituciones públicas.

4.1. Derecho a la intimidad personal y familiar (art. 18.1 CE)

El artículo 18.1 de la Constitución Española consagra el derecho fundamental a la intimidad personal y familiar, entendida como el ámbito reservado a la vida privada de la persona, libre de injerencias externas, incluidas las provenientes de los poderes públicos.

La instalación de videocámaras, sensores de seguimiento o el uso de tecnologías biométricas (como el reconocimiento facial) puede suponer una intromisión ilegítima si se realiza sin las debidas garantías legales, especialmente en espacios que, si bien son públicos, permiten la identificación individual de personas en actividades cotidianas.

El Tribunal Constitucional ha afirmado en varias ocasiones que la videovigilancia en lugares públicos no puede considerarse por sí sola una vulneración del derecho a la intimidad, salvo que permita la identificación constante de personas concretas o su seguimiento continuado sin consentimiento ni autorización.

4.2. Derecho fundamental a la protección de datos personales (art. 18.4 CE)

El artículo 18.4 CE establece que:

“La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

Este precepto constituye la base constitucional del derecho fundamental a la protección de datos personales, plenamente desarrollado por la legislación europea, en el reglamento general de protección de datos (RGPD) y a nivel nacional por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Se reconoce que toda persona tiene derecho a decidir sobre el tratamiento de sus datos, incluidos aquellos obtenidos mediante sistemas de videovigilancia, lectura de matrículas, drones o plataformas de análisis predictivo.

La aplicación de tecnologías de seguridad debe respetar los principios del tratamiento de datos recogidos en el artículo 5 del RGPD, que son:

- Deber de tratarse de forma legal, justa y transparente para el interesado (“licitud, lealtad y transparencia”).

- Han de recogerse con fines concretos, claros y legítimos, y no podrán usarse después de manera que contradiga esos fines; no obstante, según el artículo 89.1, emplear los datos personales con fines de archivo de interés público, investigación científica o histórica o fines estadísticos no se considerará incompatible con los objetivos iniciales (“limitación de la finalidad”).
- Deben ser adecuados, relevantes y limitarse únicamente a lo necesario para los propósitos para los que se recopilan (“minimización de datos”).
- Tienen que ser exactos y, cuando sea preciso, actualizarse; además, deberán adoptarse medidas razonables para corregir o eliminar sin demora aquellos datos que resulten incorrectos respecto a los fines para los que se tratan (“exactitud”).
- Han de conservarse de forma que se permita identificar a los interesados solo durante el tiempo indispensable para los fines del tratamiento; podrán mantenerse por periodos más prolongados si se destinan exclusivamente a archivos de interés público, investigación científica o histórica o fines estadísticos, de acuerdo con el artículo 89.1, siempre aplicando las medidas técnicas y organizativas adecuadas para proteger los derechos y libertades de los afectados (“limitación del plazo de conservación”).
- Se tratarán garantizando una seguridad adecuada, protegiéndolos frente a accesos no autorizados o ilícitos, así como frente a la pérdida, destrucción o deterioro accidental, mediante medidas técnicas y organizativas apropiadas (“integridad y confidencialidad”).

Además, el artículo 22 del RGPD regula las decisiones automatizadas y establece que ninguna persona podrá ser objeto de decisiones que produzcan efectos jurídicos sobre ella, basadas únicamente en un tratamiento automatizado de datos, salvo excepciones debidamente justificadas, como que dicha decisión sea necesaria para la celebración o ejecución de un contrato entre el interesado y el responsable del tratamiento; que esté autorizada por el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, siempre que se prevean medidas adecuadas para proteger los derechos y libertades y los intereses legítimos del interesado; o que se base en el consentimiento explícito del interesado.

4.3. Principios de legalidad, necesidad, proporcionalidad y control

Toda actuación policial basada en tecnologías de vigilancia debe respetar los principios generales del Derecho Administrativo y Penal, así como la jurisprudencia constitucional y europea:

- **Legalidad:** Cualquier sistema de vigilancia debe estar expresamente autorizado por una norma con rango de ley, tal como exige el artículo 53.1 CE para la restricción de derechos fundamentales.
- **Necesidad:** La utilización de medios tecnológicos debe responder a una finalidad legítima (por ejemplo, prevención del delito, seguridad vial, control de aglomeraciones)

y no debe haber otro medio menos intrusivo para lograr el mismo fin. Debe poder justificarse que la intervención era imprescindible en ese contexto.

- **Proporcionalidad:** La medida debe ser proporcional en sentido estricto, es decir, el beneficio obtenido en términos de seguridad debe superar el impacto negativo sobre los derechos fundamentales afectados. Por ejemplo, el reconocimiento facial masivo en tiempo real se considera desproporcionado salvo en situaciones excepcionales (como búsqueda de terroristas).
- **Control judicial y administrativo:** La colocación de cámaras de videovigilancia fijas por parte de las Fuerzas y Cuerpos de Seguridad del Estado y de las entidades locales deberá contar con la autorización del Delegado del Gobierno de la Comunidad Autónoma correspondiente, previa valoración e informe emitido por una Comisión presidida por el Presidente del Tribunal Superior de Justicia de esa Comunidad. La Agencia Española de

Protección de Datos (AEPD) puede también requerir evaluaciones de impacto o realizar inspecciones cuando existan indicios de un uso desproporcionado.

Además, los sistemas deben estar sometidos a mecanismos de rendición de cuentas, trazabilidad de accesos y auditorías internas o externas.

4.4. Transparencia, información y derechos del ciudadano

La ciudadanía tiene derecho a ser informada de forma clara y accesible sobre la existencia de sistemas de videovigilancia o tecnologías de tratamiento de datos en espacios públicos. Esto implica:

- Señalización visible con iconos y textos informativos.
- Indicación del responsable del tratamiento de datos (normalmente el Ayuntamiento).
- Información sobre el plazo de conservación, fines del tratamiento y derechos del interesado.

El ciudadano podrá ejercer ante el responsable del tratamiento sus derechos de:

- Acceso a sus datos (por ejemplo, grabaciones en las que pueda aparecer).
- Rectificación o supresión, si procede.
- Oposición al tratamiento, salvo excepciones.
- Limitación del tratamiento.

5. FUTURO DE LA TECNOLOGÍA POLICIAL

El futuro de la tecnología aplicada a la seguridad ciudadana se perfila como un entorno hiperconectado, automatizado e inteligente, en el que la información fluye en tiempo

real entre agentes, dispositivos, infraestructuras urbanas y centros de mando. Para la Policía Local, este escenario representa una oportunidad estratégica para optimizar su labor preventiva, mejorar la eficacia operativa y reforzar la protección de los derechos fundamentales de la ciudadanía.

A continuación, se exponen las principales tendencias tecnológicas que marcarán la evolución de la actuación policial en entornos urbanos durante la próxima década.

5.1. Cámaras corporales (bodycams)

Las cámaras corporales (body-worn cameras) son dispositivos portátiles que los agentes llevan adheridos al uniforme o chaleco y que graban vídeo y audio durante sus intervenciones. Su uso ha ido en aumento en múltiples países europeos y se está extendiendo en varias policías locales españolas, tanto por motivos operativos como de garantía jurídica.

Ventajas operativas:

- Transparencia en la actuación policial, al registrar de forma objetiva la interacción con el ciudadano.
- Prueba audiovisual directa para procedimientos administrativos o judiciales (por ejemplo, resistencia, amenazas, agresiones, denuncias falsas).
- Disuasión ante conductas agresivas, tanto por parte de ciudadanos como de agentes.
- Mejora de la formación y evaluación interna mediante el análisis de intervenciones reales.

Consideraciones legales:

- Su uso debe ajustarse al principio de proporcionalidad y estar regulado por ordenanza o instrucción municipal específica.
- El tratamiento de imágenes debe cumplir con el RGPD y la LOPDGDD, estableciendo responsables del fichero, plazos de conservación, acceso restringido y canales para el ejercicio de derechos.
- Se recomienda realizar evaluaciones de impacto de privacidad antes de su implantación.

5.2. Sensores urbanos conectados (Internet of Things - IoT)

La incorporación de sensores distribuidos por la ciudad, conectados entre sí a través de redes seguras, forma parte de los proyectos de Smart City que cada vez más municipios están desarrollando. Estos sensores proporcionan datos en tiempo real que pueden ser clave para la gestión policial.

Los sensores, como cámaras con análisis de video, radares, sensores de sonido y otros dispositivos IoT, recolectan datos sobre el entorno urbano. Estos datos son analizados

por sistemas de software y, en algunos casos, por inteligencia artificial, para identificar patrones, anomalías o eventos que requieran atención policial.

Tipologías de sensores útiles para la Policía Local:

- Sensores acústicos: detección de disparos, gritos, rotura de cristales o explosiones.
 - Sensores ambientales: detección de humo (posibles incendios), contaminación, partículas nocivas o gases tóxicos.
 - Sensores de ocupación: control del aforo en parques, playas o eventos multitudinarios.
 - Sensores de tráfico: detección de atascos, accidentes o circulación indebida.
- Aplicaciones prácticas:

- Activación automática de cámaras cercanas ante un evento detectado por sensor (por ejemplo, disparo en calle peatonal).
- El análisis de datos a largo plazo puede ayudar a identificar zonas de riesgo y patrones delictivos, lo que permite desplegar recursos policiales de manera más efectiva y prevenir la comisión de delitos.
- Apoyo a la planificación preventiva en zonas de riesgo o alta conflictividad.

5.3. Robots y sistemas autónomos

El desarrollo de robótica aplicada a la seguridad está aún en fases experimentales, pero ya existen proyectos piloto relevantes tanto a nivel internacional como nacional, que pueden ser trasladables al ámbito de la Policía Local en contextos concretos.

Posibles usos:

- Robots terrestres de patrulla autónoma: ya probados en aeropuertos, ferias o centros comerciales, pueden vigilar zonas peatonales o aparcamientos.
- Drones autónomos: capaces de realizar rutas preprogramadas y transmitir imágenes a los centros de control sin necesidad de pilotaje humano.
- Robots de desactivación de explosivos: aunque más propios de cuerpos especializados, podrían utilizarse por unidades intermunicipales en grandes ciudades.
- Interlocutores virtuales o kioscos inteligentes: que permiten al ciudadano denunciar, consultar o interaccionar con servicios policiales desde puntos públicos.

Beneficios potenciales:

- Reducción de riesgos para el personal policial en situaciones peligrosas.
- Aumento del alcance operativo sin incrementar plantilla.

- Mejora de la eficiencia en tareas rutinarias (patrullaje, vigilancia perimetral). Limitaciones actuales:
- Coste elevado y mantenimiento técnico especializado.
- Necesidad de regulación legal específica, sobre todo en relación con la autonomía de decisión y la protección de datos.
- Resistencia cultural o desconfianza ciudadana ante la robotización del espacio público.

5.4. Plataformas de mando integradas

El futuro inmediato pasa por la interoperabilidad en tiempo real de todos los sistemas tecnológicos policiales. Esto incluye cámaras, drones, sensores, bases de datos, sistemas de despacho de emergencias y comunicaciones de voz.

Las plataformas de mando y control (Command & Control) permiten a los mandos policiales:

- Recibir información multicanal geolocalizada en tiempo real.
- Gestionar los recursos desplegados mediante mapas dinámicos.
- Activar protocolos automáticos según tipologías de incidentes.
- Coordinar con otros cuerpos y servicios (Policía Nacional, Bomberos, Emergencias 112). Ventajas específicas para la Policía Local:
 - Optimización del patrullaje, mediante análisis de zonas calientes y patrones horarios.
 - Priorización de llamadas o avisos en función de la gravedad y recursos disponibles.
 - Registro unificado de actuaciones, útil para informes, estadísticas o auditorías.
 - Mejora de la seguridad del agente en intervenciones complejas (botón de alerta, ubicación exacta, comunicación inmediata).

6. CONCLUSIÓN

El análisis detallado de las tecnologías aplicadas a la seguridad ciudadana revela que nos encontramos ante un proceso de transformación profunda que está redefiniendo el trabajo diario de las Policías Locales. La implementación de sistemas de videovigilancia, el despliegue de drones, la adopción de soluciones de inteligencia artificial y big data, junto con la integración de sensores urbanos, robots y plataformas de mando avanzadas, configuran un nuevo escenario operativo caracterizado por la digitalización, la inmediatez y la interconexión de la información.

Esta evolución tecnológica ofrece innegables ventajas: desde la capacidad de anticiparse a situaciones de riesgo mediante la vigilancia predictiva, hasta una intervención más rápida y eficaz ante emergencias, la obtención de pruebas audiovisuales para procedimientos judiciales o la mejora de la transparencia y confianza ciudadana. Herramientas como las cámaras corporales, los drones con cámaras térmicas o la lectura automática de matrículas permiten ampliar el alcance de la vigilancia, reforzar la presencia policial en zonas críticas y optimizar la gestión de recursos.

Sin embargo, junto a las oportunidades aparecen también importantes retos y responsabilidades. La tecnología, por sí sola, no puede sustituir el juicio humano, la cercanía al ciudadano, ni el sentido ético que debe guiar la actuación policial. Resulta esencial garantizar que el uso de estas herramientas respete los principios constitucionales y legales: legalidad, necesidad, proporcionalidad, control y transparencia. Solo así se puede preservar el equilibrio entre la eficacia operativa y la protección de derechos fundamentales como la intimidad, la protección de datos personales o la libertad de circulación.

El marco normativo español y europeo, reflejado en la Ley Orgánica 4/1997, el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018 y el reciente Reglamento de Inteligencia Artificial de 2024, proporciona las garantías necesarias para un uso responsable de estas tecnologías. Pero es imprescindible que las Policías Locales no solo conozcan estas normas, sino que además desarrollen protocolos internos claros, realicen evaluaciones de impacto en privacidad, formen de manera continua a sus agentes y fomenten la participación y la información ciudadana para mantener la confianza pública.

El futuro de la Policía Local pasa por convertirse en un actor clave dentro de un modelo de ciudad inteligente y segura, donde las decisiones se apoyan en datos, la coordinación es más ágil y la capacidad de respuesta se multiplica gracias a la tecnología. Pero, al mismo tiempo, debe seguir siendo una policía cercana, preventiva y comunitaria, que entienda la seguridad no solo como control, sino también como garantía de convivencia, cohesión social y respeto a la dignidad de las personas.

En definitiva, la innovación tecnológica debe ser siempre una aliada, nunca un fin en sí misma. Su éxito dependerá de que sepamos integrarla de forma ética, proporcional y transparente en la labor diaria, poniendo siempre en el centro a la ciudadanía y la protección de sus derechos.

7. BIBLIOGRAFÍA

Legislación española

- Constitución Española (1978). Boletín Oficial del Estado (BOE), núm. 311, de 29 de diciembre de 1978.

- Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. BOE núm. 186, de 5 de agosto de 1997.
- Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 4/1997. BOE núm. 93, de 19 de abril de 1999.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 6 de diciembre de 2018.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. BOE núm. 126, de 27 de mayo de 2021.
- Real Decreto 517/2024, de 4 de junio, por el que se desarrolla el régimen jurídico para la utilización civil de sistemas de aeronaves no tripuladas (UAS), y se modifican diversas normas reglamentarias en materia de control a la importación de determinados productos respecto a las normas aplicables en materia de seguridad de los productos; demostraciones aéreas civiles; lucha contra incendios y búsqueda y salvamento y requisitos en materia de aeronavegabilidad y licencias para otras actividades aeronáuticas; matriculación de aeronaves civiles; compatibilidad electromagnética de los equipos eléctricos y electrónicos; Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea; y notificación de sucesos de la aviación civil. BOE núm. 136, de 5 de junio de 2024.

Normativa europea

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea (DOUE) núm. 119, de 4 de mayo de 2016.
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. DOUE L 119, de 4 de mayo de 2016.
- Reglamento de Ejecución (UE) 2019/947 de la Comisión, de 24 de mayo de 2019, relativo a las normas y procedimientos aplicables a la utilización de aeronaves no tripuladas. DOUE L 152, de 11 de junio de 2019.
- Reglamento Delegado (UE) 2019/945 de la Comisión, de 12 de marzo de 2019, sobre sistemas de aeronaves no tripuladas y operadores de terceros países. DOUE L 152, de 11 de junio de 2019.

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) DOUE L 1689, de 12 de julio de 2024.

Documentos y directrices técnicas

- Agencia Española de Protección de Datos (AEPD). Guía sobre el uso de videocámaras para seguridad y otras finalidades. Madrid: AEPD.
- Comité Europeo de Protección de Datos (CEPD). Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley.
- Ministerio del Interior. Normativa de UAS/drones.

LA GRABACIÓN DE IMÁGENES DE LA **POLICÍA LOCAL** EN LAS INTERVENCIONES POLICIALES



AUTOR: RUBÉN FOSELA ROMÁN.

LA GRABACIÓN DE IMÁGENES DE LA POLICÍA LOCAL EN LAS INTERVENCIONES POLICIALES

Autor: Rubén Fosela Román

PRÓLOGO.

Desde la introducción de los teléfonos móviles en España a mediados de los años 90 es cuando empieza a proliferar la venta de estos aparatos y se inicia su expansión y uso por millones de usuarios. A partir del año 2004, con la aparición de la banda ancha, se consigue no sólo un aumento de la velocidad de internet sino la mejora de muchas características de los terminales móviles, haciendo de este modo, un atractivo añadido para los usuarios.

En el año 2013 se inicia otro salto de calidad en el uso de los móviles, apareciendo en el mercado el sistema 4G, llegando a incrementarse la calidad de éstos en cuanto al uso y la transmisión de datos, fotografías, videos, streaming, etc., así como el uso compartido entre los usuarios. Hoy en día ya está plenamente instalada y en funcionamiento la tecnología 5G, todavía más rápida, eficaz e interactiva que la anterior, logrando una conectividad ultrarrápida. Todo ello hace que los usuarios con sus teléfonos inteligentes realicen fotografías y videos y los compartan en tiempo real con una gran cantidad de personas, permitiendo el envío de todo tipo de archivos multimedia.

Consecuentemente, esta tecnología muy útil para todos, a veces es utilizada por aquellos que se creen poseer todos los derechos y que, precisamente son en su mayoría los que están cometiendo las infracciones o delitos; también los hay que graban por el hecho de ver a un policía realizando su trabajo, por si comete alguna “ilegalidad”. Hoy en día, la Administración graba (cámaras de vigilancia en lugares estratégicos, cámaras de bancos, controles de accesos, control del tráfico, etc.), las empresas graban (bancos, museos, joyerías, etc.) y los particulares, también realizan grabaciones de videos y toman imágenes de ocio o de cualquier percance que les suceda o que sean testigos. Todo esto forma parte de lo que se puede denominar la “cultura de la vigilancia”, todos graban a todos. Y parece ser, que está de moda grabar cualquier actuación de la Policía, lo que a veces interfiere en la labor de éstos al sentirse intimidados y, a veces, coaccionados; parece que los agentes están sometidos al libre albedrío e impunidad de cualquier individuo que pase a su lado y que quiera grabarlo para compartirlo.

Por ello, debido a la constante puesta en entredicho de la labor policial al ser objetivos de aquellos que piensan que se actúa siempre abusando del ciudadano (de sus derechos), se elabora este trabajo de ayuda a los profesionales de la Policía Local, con el fin de poder servir de consulta de la actual legislación y de las posibles infracciones y vulneraciones del ordenamiento jurídico por parte de aquéllos que quieren dejar constancia de la actuación de turno. No sólo se graban imágenes o videos, sino también las publican en las redes sociales, incrementándose el uso de Whatsapp o Telegram por su fácil uso y extensa expansión en todos los terminales móviles.

Este modesto trabajo de investigación denominado LA GRABACIÓN DE IMÁGENES DE LA POLICÍA LOCAL EN LAS INTERVENCIONES POLICIALES, se publica en

cooperación con el sindicato SIP-AN, para ser distribuido en su versión libro a los profesionales de la seguridad pública que estudian las diferentes acciones formativas en esta materia, así como en la versión de publicación en línea, que ha sido subida a la red en el Área de Formación (Biblioteca Virtual) de la página web del sindicato reseñado (www.sip-an.es).

ÍNDICE

1. INTRODUCCIÓN
2. LA LEY ORGÁNICA 1/1982, DE PROTECCIÓN CIVIL DEL DERECHO AL HONOR, A LA INTIMIDAD PERSONAL Y A LA PROPIA IMAGEN.
3. EXTRACTOS DE SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL
 - 3.1 La sentencia del Tribunal Constitucional número 156/2001, de 2 de julio.
 - 3.2 La sentencia del Tribunal Constitucional número 72/2007, de 16 de abril
 - 3.3 Sentencias en contra de la grabación de imágenes de policías
 - 3.3.1 La Sentencia 113/2006, de 31 de marzo, de la Audiencia Provincial de Burgos (apelación de juicio de faltas en la que se absuelve al policía de la falta de coacciones)
 - 3.3.2 La sentencia 120/2008, de 11 de marzo, de la Audiencia Provincial de Madrid (recurso contra juicio de faltas en la que se procede a la absolución de un policía de la falta de coacciones)
4. LA DISCUTIDA INFRACCIÓN CONTENIDA EN EL ARTÍCULO 36.23 DE LA LO 4/2015, DE 30 DE MARZO
5. LAS INFRACCIONES CONTENIDAS EN LOS ARTÍCULOS 72, 73 Y 74 DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS, 3/2018, DE 5 DE DICIEMBRE, ASÍ COMO DEL REGLAMENTO DE LA UE 2016/679, DE 27 DE ABRIL 12
6. EL ARTÍCULO 197 DEL CÓDIGO PENAL
7. CONCLUSIONES.
8. BIBLIOGRAFÍA Y WEBGRAFÍA

1. INTRODUCCIÓN.

Últimamente es muy común observar en las redes sociales (Facebook, Instagram y, sobre todo, Whatsapp y Telegram) cómo algunos individuos en el transcurso de una actuación

policial sin importancia, graban a los agentes, ya sea en video o en imágenes. Casi todos ellos, aun mediando la oposición del agente de la autoridad. Es paradójico que, según los videos de estas intervenciones, cuanto más le dicen los agentes que cesen en su actitud, más inciden en ello, yo diría, con más vehemencia, constituyendo en sí mismo y por la forma que emplean (grabando en la cara del agente, haciendo caso omiso, insultando, menospreciando, etc.) una falta de respeto hacia los intervinientes constitutiva de la infracción del artículo 37.4 de la Ley Orgánica 4/2015, de 30 de marzo, sobre Protección de la Seguridad Ciudadana, (referente a las faltas de respeto hacia los agentes de las fuerzas y cuerpos de seguridad y cuando estén ejerciendo sus funciones de protección de la seguridad ciudadana -sólo en los casos que no sean constitutivas de infracción penal tales como amenazas, desobediencias graves, atentados, injurias o calumnias graves).

Están en juego distintos tipos de normas que afectan al controvertido asunto y que pueden utilizar los policías en su defensa, con objeto de denunciar (e incautar los instrumentos utilizados) a este tipo de personas que se creen poseer todos los derechos en detrimento de los nuestros. Como punto de partida, señalaremos el artículo 18.1 de la Constitución Española:

Sin entrar en valoraciones, no dice nada qué clase de personas son titulares de este derecho, por tanto, se aplica a todo el mundo, a todas las personas que residan o deambulen por este país llamado España, policías incluidos.

2. LA LEY ORGÁNICA 1/1982, DE PROTECCIÓN CIVIL DEL DERECHO AL HONOR, A LA INTIMIDAD PERSONAL Y A LA PROPIA IMAGEN.

El artículo 1 garantiza directamente el derecho fundamental al honor, a la intimidad personal y familiar y al a propia imagen (artículo 18 de la Constitución Española) y continúa diciendo que serán protegidos cuando estén sometidos a intromisiones no legítimas y de acuerdo a lo dispuesto en esta ley.

Además, continúa exponiendo que este derecho es irrenunciable, inalienable e imprescriptible y que la debida protección del mismo quedará delimitada por las leyes y por la costumbre.

Según el artículo 7 de esta ley, reseña que tendrán la consideración de intromisiones ilegítimas, las siguientes:

1. Colocar aparatos de escucha o micrófonos, cámaras de video-vigilancia o filmación, de dispositivos ópticos u otros aparatos que sean usados para grabar y/o reproducir la intimidad o vida privada de los ciudadanos.
2. Divulgar o publicar hechos relativos a la vida privada de una persona o familia que afecten a su prestigio o fama, así como la publicación o vulneración del contenido de cartas u otros escritos personales de carácter completamente privado.

3. Tomar fotografías, grabar video o por medio de cualquier herramienta capaz de reproducir, de la imagen de la vida particular de una persona.

En contraposición a ello, el artículo 8 de la ley se expresa argumentando que no se considerarán intromisiones ilegítimas aquellas actuaciones debidamente autorizadas por la Autoridad que sea competente, de acuerdo a lo dispuesto en la ley, ni tampoco cuando sea de aplicación un interés histórico, científico o cultural notable.

Sin embargo, este derecho a la propia imagen no impide:

a) Tomar fotografías o grabar videos de secuencias de la vida diaria o sucesos de interés, cuando se trate de personas con alcance público (alcalde, concejal, ministro, consejero...) o una profesión con una proyección pública (policía, bombero, cartero...) y estas imágenes o videos sean tomadas durante un acto de trascendencia pública o en medio de la calle.

b) Es lícito realizar caricaturas de estas personas (por dibujantes profesionales), en base a los usos sociales (muy usado y publicado en los periódicos y revistas más importantes).

c) También es adecuado a la norma cuando la información gráfica sobre un suceso o acaecimiento público cuando la imagen casual de una persona aparezca en la imagen o video como meramente accesorio.

Lo reseñado anteriormente no resulta aplicable a la toma de imágenes en relación con las autoridades, funcionarios o ciudadanos que realicen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza (no es descabellado pensar que nosotros, los policías, podemos necesitar ese anonimato debido a nuestra profesión, que es de riesgo, más aún cuando la mayoría de estas grabaciones son realizadas a poco más de un metro de los agentes), como pueden ser los policías judiciales que necesitan de este anonimato para ejercer adecuadamente sus funciones de averiguación e investigación de hechos criminales.

Según algunas interpretaciones y en base a lo expuesto, la captación de la imagen de un policía durante un acto público o lugar abierto al público no está protegido por el derecho a la propia

imagen. Al parecer según algunos demagogos eruditos, los policías no tenemos el derecho de ejercer por la vía civil el derecho al honor, a la intimidad personal y a la propia imagen, no podemos denunciarlo en el Juzgado de Primera Instancia. En este rango, aunque con matices, hay doctrina del Tribunal Constitucional, especialmente la Sentencia número 72/2007, de 16 de abril, la cual negaba el amparo constitucional a una policía cuya imagen había sido publicada en un periódico con ocasión de un violento desalojo de viviendas (el caso de la Sargento de la Policía Municipal de Madrid, aunque en este caso la publicación de la imagen de ésta se hizo en un periódico, por tanto, hay

en juego un derecho a la información [art. 20 CE] y es más fácil ponderar los derechos en juego en detrimento de la imagen del policía).

3. EXTRACTOS DE SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL.

Analizadas las diferentes sentencias del Tribunal Constitucional sobre el asunto de la grabación de imágenes por los particulares, enumeramos las siguientes por ser más relevantes:

3.1 La sentencia del Tribunal Constitucional número 156/2001, de 2 de julio.

El derecho a la propia imagen es un derecho fundamental que protege la facultad de una persona para controlar la captación y difusión de sus rasgos físicos, considerándose también que son derechos fundamentales que garantizan la libertad de expresar y difundir pensamientos, ideas e información. La ponderación y aplicación de estos derechos es un principio jurídico que implica evaluar y equilibrar los derechos en conflicto, teniendo en cuenta su importancia y las circunstancias de cada caso. Asimismo, el interés público puede justificar la captación o difusión de la imagen de una persona, especialmente cuando se trata de información relevante para la sociedad. En resumen, el texto destaca la necesidad de equilibrar el derecho a la propia imagen con las libertades de expresión e información, mediante una ponderación cuidadosa de los intereses en juego en cada caso concreto.

3.2 La sentencia del Tribunal Constitucional número 72/2007, de 16 de abril.

Se profundiza en la aplicación del artículo 8.2 a) de la Ley Orgánica 1/1982, que regula la protección del derecho a la propia imagen, en el contexto de una persona que ejerce un cargo público. En referencia a aquellas personas que ostenten un cargo público, se diferencia que la persona cuya imagen fue captada ejercía un cargo público, específicamente como Sargento de la policía municipal de Madrid, resulta crucial, ya que el ejercicio de un cargo público puede limitar el alcance del derecho a la propia imagen. Se añade que la fotografía de un particular fue tomada durante un acto público: un desalojo por orden judicial. La intervención de la policía municipal de Madrid fue necesaria debido a la resistencia violenta de los afectados, concretamente se llevó a cabo en una calle de un barrio madrileño, un espacio público. Este factor también es relevante para determinar la aplicabilidad del artículo 8.2 a). Continúa la sentencia argumentando que hay excepciones al derecho a la propia imagen, permitiendo su captación o difusión cuando se trata de personas que ejercen un cargo público y la imagen se tome durante un acto de carácter público o en la calle o parque público. Para concluir, la sentencia estudiada justifica, en este caso, la captación y difusión de la imagen de una persona que ejerce un cargo público, basándose en que la fotografía fue tomada durante un acto público y en un lugar público, lo que se ajusta a las excepciones establecidas en el artículo 8.2 a) de la Ley Orgánica 1/1982.

3.3 Sentencias en contra de la grabación de imágenes de policías.

Existen sentencias que resuelven en contra de la grabación de imágenes de agentes por particulares (con el teléfono móvil), sin motivo alguno, entre otras, destacamos las siguientes:

3.3.1 La Sentencia 113/2006, de 31 de marzo, de la Audiencia Provincial de Burgos (apelación de juicio de faltas en la que se absuelve al policía de la falta de coacciones).

Menciona y alude esta sentencia que el artículo 18.1 de la CE garantiza el derecho a la intimidad personal. Y continúa diciendo que una sentencia de la Sala 1ª del Tribunal Supremo (Sala de lo Civil), en referencia a este derecho, dice que el policía tenía el derecho, como el resto de los ciudadanos, a su propia imagen y de disponer de ella a efectos de poder ser identificado. Por lo tanto, es muy posible que, debido a ello, la persona pueda ser reconocida por sus rasgos físicos que son únicos, que se transgrede por el simple hecho de tener notoriedad pública (la persona grabada), argumentándose que esta persona tiene el derecho de impedir la reproducción y/o publicación de su imagen que ha sido tomada por una persona sin autorización (sentencias del Tribunal Constitucional 81/2001, de 26 de marzo y 156/2001, de 2 de julio).

Es decir que no existe en principio un derecho de captar mediante cualquier sistema técnico de reproducción imágenes de personas. La cuestión que aquí se plantea es de si un particular puede fotografiar a las Fuerzas y Cuerpos de Seguridad, en este caso Policías Municipales de Burgos cuando intervienen en un lugar público en razón de su cargo, o si, tal y como sostiene la sentencia recurrida, esta actuación del particular no afecta a la esfera privada de las personas. Continúa aún más claro esta sentencia argumentando que no comparte este Tribunal la argumentación que propugna el Juez a quo, ya que a la luz de la doctrina del Tribunal Constitucional reflejada en el fundamento de derecho no existe un derecho para obtener imágenes de una persona por medios que posteriormente permitan su posterior difusión sin su consentimiento. Como excepción establece que esta restricción se vería limitada cuando se trate de evitar o descubrir hechos delictivos o de acontecimientos de interés público y esta actuación se realice al amparo del derecho fundamental de comunicar libremente información veraz, reconocido en el artículo 20.1 d) de la Constitución, supuesto en el debería ponderarse cuál de los dos derechos fundamentales debía prevalecer en su protección, pero ello no ocurre en el supuesto sometido a enjuiciamiento toda vez que el denunciante no pertenecía, como ya se ha dicho, a ningún medio de comunicación. Y continúa la sentencia (resumida): Una vez determinado que la actuación de la persona que denuncia por tomar fotografías a los policías locales que desempeñaban sus funciones y trataban de actuar y contrarrestar el orden alterado, y que lo hacían sin llevar los actuaban sin llevar los rostros ocultos, no estaba amparada legalmente al hacerse sin su consentimiento, el requerimiento para que entregase la cámara fotográfica era totalmente ajustado a derecho, ya que este agente no sabía el posible uso que de esas imágenes de los agentes pudiera hacer el denunciante. Por ende, los agentes actuantes tomaron las correspondientes medidas de seguridad con el único objeto de impedir que sus imágenes fuesen distribuidas por internet, por lo que la orden dada para entrega inmediata de la cámara fue declarada totalmente legal.

3.3.2 La sentencia 120/2008, de 11 de marzo, de la Audiencia Provincial de Madrid (recurso contra juicio de faltas en la que se procede a la absolución de un policía de la falta de coacciones).

Esta sentencia se desenvuelve en los mismos términos que la anterior. Alega el recurrente la falta de tipicidad (falta de coacciones, antiguo artículo 620.2 del Código Penal) de los hechos acaecidos, ya que la persona denunciante realizó fotografías de los agentes de la Policía Municipal de Madrid sin su consentimiento, por ello, la orden dada por estos agentes para que borrara las imágenes captadas era legal, pues estos agentes desconocían el posible uso que el denunciante iba a dar a esas fotografías, y por más que evidentes razones de seguridad trataron de preservar su imagen, y dado que el testigo y denunciante no accedió al borrado de esas fotografías (que comprometían la seguridad de los agentes), se considera legal y reglamentada la intervención del teléfono móvil que portaba el denunciante de los hechos. Se añade que no estamos ante un conflicto entre el derecho a inherente de las personas y el propio derecho a la información, pues no se trata de imágenes o fotografías hechas por un medio de comunicación, sino por un particular. Sobre la cuestión planteada debe señalarse que el derecho a la propia imagen es el derecho que cada individuo ostenta como propio para que las demás personas no reproduzcan su cara, su cuerpo o su imagen completa sin su consentimiento, de tal manera que cualquier captación de estas imágenes, ya sea mediante fotos o vídeos u otros procedimientos usados para captar la imagen absolutamente privada de una persona o, incluso, fuera de ella, puede infringir directamente el derecho fundamental a la imagen. El derecho a la propia imagen que todos tenemos viene consagrado en el artículo 18.1 de la CE, no obstante, el apartado 5 del artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, propugna como una intromisión no autorizada y vulneradora de este derecho cuando se realizan las siguientes acciones por una persona no autorizada:

a) Tomar fotografías o grabar video o mediante cualquier otra herramienta similar, la cara o imagen de personas durante el desempeño de su vida íntima o familiar.

b) También realizar lo anterior cuando los sujetos grabados estén en la vía pública, salvo las excepciones previstas en el artículo 8, apartado 2 de la misma norma.

c) Esta excepción que grabar a las personas y, por consiguiente, ese derecho a la propia imagen no obstaculiza o no impide grabarlos cuando:

I. Estas grabaciones sean de personas que desempeñan un cargo público o una profesión con alcance y relevancia pública (alcaldes, concejales, ministros, policías, bomberos, etc.). No será aplicable cuando estas personas, ya sean funcionarios (policía, investigadores judiciales, jueces, fiscales, agentes de aduanas, etc.) necesiten no ser identificados para que no obstaculicen estas grabaciones en el desempeño normal y con seguridad de sus labores profesionales.

II. Y es necesario que estas grabaciones o imágenes se tomen durante un acto público o en las zonas o lugares públicos (una plaza, una calle, ayuntamiento, etc.).

III. Cuando un reportero, fotógrafo o periodista capte una imagen pública de cualquier acto o lugar público y salga la imagen de una persona de forma casual y no buscada.

En base a ello, como conclusión es que esta apelación debe ser aplicable, ya que se analiza en esta sentencia un posible conflicto existente entre el derecho al a propia imagen que todos tenemos (incluidos los policías) y su contraposición con el derecho a la información a la que todos también tenemos derecho. Y ello se debe cuando la persona que realiza la grabación no pertenece a un medio acreditado de información, ya sea periódico, radio o televisión, por tanto, carece de acreditación y legitimación alguna y, para más inri, la noticia de grabar a un policía durante una actuación rutinaria no tiene interés de la población o dicho interés público es nulo o baladí.

Esta sentencia está fundamentada en la STC de 23 de mayo de 2007 acerca de una fotografía publicada referida a una fotografía que se hizo pública en el periódico Diario 16 donde se podría observar a una Policía Municipal de Madrid durante la desocupación de una finca que había sido usurpada. No obstante, en el caso de la sentencia analizada se trata de una persona no acreditada, que no es periodista, que obtuvo varias fotografías de la actuación policial de varios agentes municipales relacionada con la retirada de un turismo de la vía pública con la grúa municipal; se deduce por cualquier persona que estas grabaciones no tienen ni el más mínimo interés como para ser publicado en un medio de comunicación.

4. LA DISCUTIDA INFRACCIÓN CONTENIDA EN EL ARTÍCULO 36.23 DE LA LO 4/2015, DE 30 DE MARZO.

El artículo 36. 23 de esta ley define como infracción lo siguiente: El uso no autorizado de imágenes personales o profesionales de las autoridades o miembros de las Fuerzas y Cuerpos de Seguridad (Estado, CC.AA. o Locales) que pueda comprometer la seguridad personal o familiar de los agentes, de las instalaciones en resguardo o amenazar el éxito de una operación, respetando el derecho fundamental a la información. Se dio inicio por medio de la Instrucción 13/2018, de 17 de octubre, de la Secretaría de Estado de Seguridad, referente a la grabación de imágenes: Para que los hechos constituyan una infracción de seguridad es esencial que se utilicen las imágenes o la información personal o profesional de los agentes, las instalaciones que están protegidas o las operaciones policiales, y que ese uso ponga en riesgo la seguridad personal de los agentes o de sus familias, de las instalaciones en resguardo o el éxito de una operación.

Por lo tanto, esta situación de riesgo o peligro debe estar reflejada en el acto o denuncia o, en su caso, en los informes anexos adecuados, donde se detallará con e mayor nivel de especificidad posible, el peligro o riesgo ocasionado y los factores que lo han generado.

En consecuencia, no se considera infracción la simple toma de imágenes o el tratamiento de los datos de los agentes si esto no representa un riesgo o peligro para ellos, sus

familiares, las dependencias e instalaciones policiales o las actuaciones policiales importantes. En esos últimos casos, los agentes involucrados deberán actuar en cada situación de acuerdo con las normativas de seguridad y autoprotección, materias clasificadas, protección de datos personales, así como las disposiciones penales o civiles aplicables, según corresponda. Todo esto, sin perjuicio de la posibilidad de identificar a la persona que haya capturado las imágenes con el objetivo de proceder, en su caso, a la realización de las actuaciones pertinentes para salvaguardar los derechos de las personas involucradas o proponer, en su caso, para sanción administrativa al artículo 36.23 de la LOPSC o penal (artículo 197 del CP) si se pretendiera hacer un uso irregular de estos datos o imágenes de igual manera que se ha reseñado anteriormente.

Asimismo, la nota informativa número 108/2020, del Tribunal Constitucional, dictaminó que el término “no autorizado” incluido en el artículo 36.23 de la LOPSC no estaba adaptado a la CE, proponiendo una nueva dimensión y entendimiento de dicho artículo, destacando que la palabra “uso” se debía interpretar, para que se pudiera denunciar por este hecho como infracción grave, que no bastaba con la captación o grabación de video de los agentes, sino que, además, estas grabaciones deberían ser publicadas (de forma ilegal) utilizando las múltiples redes sociales de las que hoy en día se dispone.

En base a ello, haciendo un análisis pormenorizado de este precepto, se hace patente que para que se infrinja lo estipulado en el mismo se hace necesario lo siguiente:

- a) La toma de estas imágenes por cualquier persona de una actuación policial de los agentes de policía (cosa que gusta mucho, sobre todo, a los infractores reincidentes).
- b) Y que estas grabaciones puedan poner en peligro la seguridad de los agentes, familiares o las instalaciones de la Policía o, incluso, poner en peligro una importante actuación policial.
- c) Pero no sólo basta lo anterior, sino que, para más inri, y muy a pesar de los miembros de las fuerzas y cuerpos de seguridad (favoreciendo de este modo a aquellas personas que se creen estar por encima de todo y de todos), se tiene que dar el requisito último de la publicación de las imágenes de los agentes (o instalaciones policiales).

Esta interpretación del Alto Tribunal deja la puerta abierta para ponderar el equilibrio entre el derecho a la intimidad personal y el de información (este último poco aplicable a los que nos graban en la calle, ya que no suelen ser periodistas) y hace más difícil, si cabe, la actuación de los miembros de la Policía que no tienen otra misión que salvaguardar y proteger los derechos de los ciudadanos.

5. LAS INFRACCIONES CONTENIDAS EN LOS ARTÍCULOS 72, 73 Y 74 DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS, 3/2018, DE 5 DE DICIEMBRE, ASÍ COMO DEL REGLAMENTO DE LA UE 2016/679, DE 27 DE ABRIL.

En base a lo establecido en el artículo 6 de la LOPD y en el 4.11 del Reglamento de la UE, se entiende por consentimiento del afectado cuando éste manifiesta de una forma libre

y voluntaria, además de inequívoca, que acepta mediante la firma de un documento una declaración afirmativa en la que acepta que se traten sus datos personales por el director del tratamiento de datos. Hoy en día, se firman estos documentos en cualquier afiliación a asociación, partido político, realización de un contrato de cualquier índole, aceptando grabaciones de los niños en el colegio, hermandad, etc.

Ni que decir tiene, que aquellas personas que intentan grabar a la Policía Local no ostentan, sin ningún género de dudas, nuestro consentimiento, por ello, el infractor empieza a serlo desde el principio y es que, además de poder infringir el artículo 36.23 de la LOPSC puede vulnerar también lo establecido en el 37.4 de la misma norma por faltar al respeto a los agentes que realizan la actuación. Sirva de ejemplo las grabaciones que pululan por las redes sociales en las que el infractor le pone en la misma cara de éstos el móvil a la par que le faltan al respeto de forma verbal, creyéndose al mismo tiempo poseedores de todos los derechos establecidos en detrimento, como siempre, de los agentes que son o somos quienes debemos defender al resto de los ciudadanos, precisamente de estos energúmenos.

El artículo 6.1.a del Reglamento estudiado expone que el tratamiento de datos personales SOLO SERÁ LÍCITO SI EL INTERESADO DIO SU CONSENTIMIENTO para el tratamiento de sus datos personales.

¿Qué se consideran datos de carácter personal?
El artículo 3.a) de la antigua LOPD (LO 15/1999, de 13 de diciembre), concretaba el concepto de DATOS DE CARÁCTER PERSONAL como cualquier dato o información relativa a las personas identificadas o que puedan resultar identificadas. Y la letra c) del mismo artículo definía el TRATAMIENTO DE DATOS como el conjunto de operaciones y procedimientos de carácter automático (aunque no es necesario) que puedan aceptar recoger, grabar y archivar, así como permitirá la modificación y la cancelación de los mismos y, en última instancia, la cesión de estos datos cuando sean necesarios para establecer las consultas o comunicaciones entre entes. Del mismo modo, el artículo 5, apartado 1.f) del RD 1720/2007, de 21 de diciembre, reglamento de desarrollo de la LOPD (LO 15/1999, de 13 de diciembre, en vigor) define los DATOS DE CARÁCTER PERSONAL como cualquier clase de información numérica (entre ellas, las matrículas de los coches, DNI, NIE, números de la Seguridad Social, etc.), alfabética, imágenes o videos, grabaciones de voz o de cualquier otra herramienta que sea capaz de captar a personas físicas identificadas o que puedan serlo.

Además, el artículo 22 de la LOPD, expone que solo podrán captarse imágenes de los entorno públicos, fuera de la vida privada y familiar de las personas, sólo si resulta imprescindible para preservar y proteger la seguridad colectiva así como de los bienes y de sus instalaciones con FINES DE VIDEOVIGILANCIA, obligando a la persona particular que graba las imágenes de terceras personas el deber de información de los afectados

atendiendo al ejercicio de los derechos de acceso, supresión y oposición al tratamiento. Deben, además, disponer del famoso cartel de la Agencia Española de Protección de Datos.



Cartel obligatorio en las zonas videovigiladas.

Por todo lo anterior, si nos encontramos en nuestra labor diaria en una actuación en la que nos graben sin nuestro consentimiento, pueden incurrir en infracciones administrativas ya que el derecho en cuestión (a la propia imagen) está protegido, en principio y sin análisis de la procedencia de otras normas conexas, por los preceptos de la norma estudiada, esto es, la Ley Orgánica 3/2018, de 5 de diciembre (artículos 72.1.b), 73.c) y 74.a) y c)), de Protección de Datos Personales y garantía de los derechos digitales, así como del Reglamento de la UE número 2016/679, relativo a la protección de los datos personales.

Y en directa relación con el informe jurídico número 0077/2013 de la Agencia Española de Protección de datos, sobre la captación por particulares de la imagen de los empleados públicos, bien tomadas mediante fotos o por videos, generalmente a través de teléfonos móviles sin consentimiento de los interesados en el que se considera que la mera captación de la imagen de un empleado público supone un tratamiento de datos, es por lo que en aplicación del artículo 11.1.a de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, por la que se exige a los agentes de la autoridad debemos “Velar por el cumplimiento de las leyes y disposiciones generales”, por ello, estaremos facultados para proceder a la denuncia de los hechos.

La dudosa intervención del móvil por inseguridad de los agentes.

La aprehensión de estos efectos tiene su soporte legal en el artículo 19.2 de la Ley Orgánica 4/2015, de 30 de marzo, de Seguridad Ciudadana:

- a) Se intervendrán las drogas tóxicas, armas u otros efectos procedentes de la comisión de un delito o infracción administrativa.
- b) Se reflejará esta incautación en un acta redactada al efecto que deberá ser firmada por el infractor y por los policías actuantes en calidad de instructor y secretario. En caso de negarse, se hará constar esta circunstancia en el apartado de firmas de dicha acta.
- c) Por último, salvo que se contante una prueba en contra, este acta gozará al igual que la denuncia que se extienda, de presunción de veracidad.

En relación a ello, el artículo 47.1 de la misma ley destaca que los agentes intervinientes deberán intervenir de forma cautelar los instrumentos usados para las infracciones cometidas, también el dinero en efectivo, así como los objetos y productos obtenidos. Esta intervención cautelar (sus objetos intervenidos) deberá ser custodiada en las dependencias de las fuerzas y cuerpos de seguridad a la par que se tramita el expediente administrativo sancionador, ya que se puede resolver por la autoridad competente, la devolución o, en su caso, el decomiso efectivo para su destrucción.

Por lo expuesto, la intervención del móvil del que hacen uso estos infractores es ajustada a Derecho. Y, por si fuera poco, también amparada en los artículos 56.2 y 56.3.i de la Ley 39/2015, de

1 de octubre, de Procedimiento Administrativo Común, al considerarse EFECTOS PROCEDENTES DE INFRACCIÓN ADMINISTRATIVA, teniendo su aprehensión la finalidad de servir como medio de prueba de la comisión de la infracción, evitar la comisión de nuevas infracciones, sirviendo así para la protección personal de los intereses implicados de forma que permita asegurar la efectividad de la resolución que en su caso pudiera recaer por parte del órgano sancionador.

6. EL ARTÍCULO 197 DEL CÓDIGO PENAL.

Estos hechos también pueden ser constitutivos de un delito contra la intimidad y el derecho a la propia imagen. Este delito está enmarcado dentro del Título X, denominado delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio y dentro del capítulo I, Del descubrimiento y revelación de secretos se erige este artículo. El núcleo fundamental o bien jurídico protegido es la intimidad personal, consagrado como se ha repetido en el artículo 18.2 de nuestra CE. Se castiga a quién transgreda la intimidad de otra persona, sin el consentimiento de ésta o bien se apropie de sus documentos, ya sean en papel, cartas o emails, así como interceptar sus comunicaciones en la red (internet). Establece y condiciona este artículo diferentes penas según la intensidad, perjuicio o violación de esta intimidad personal, ponderando las penas en los diferentes tipos, tanto el básico como los agravados.

Si durante una intervención policial cualquier individuo que empiece a grabar a los agentes de la Policía Local sin su consentimiento y durante la misma profiere frases como: te vas a enterar, te voy a sacar en Youtube e Instagram, voy a hacer que todo el mundo sepa quién eres, ya te tengo identificado, sabemos quién eres, etc., denota, como no podría ser menos, una falta de motivación racional sobre la finalidad de la captación de las imágenes.

Todo esto nos autoriza para intervenir el material usado para la grabación (artículo 19.2 LOPSC). Y si esta norma nos impide actuar hasta que el particular publique las grabaciones, la Sentencia 113/2006, de 30 de marzo, de la Audiencia Provincial de Burgos, alegó que la obtención de fotografías de los agentes para un uso posterior ignorado NO ES UN ACTO LEGÍTIMO AL NO MEDIAR CONSENTIMIENTO de los afectados...

Es más, el artículo 197 del Código Penal califica como delictiva la conducta de aquellas personas (sujetos activos del delito) quienes para vulnerar la intimidad de otra use herramientas de grabación de imágenes, por lo que la decisión de impedir un eventual delito está amparada por la circunstancia eximente de la responsabilidad penal del artículo 20.7 del Código Penal. En nuestro caso se podría intervenir el móvil, realizar el acta de intervención del mismo y realizar diligencias por posible infracción penal.

Para concluir, el artículo 588 sexies c. autorización judicial de la LECrim., en el apartado 4 se establece de forma resumida en relación a lo anteriormente expuesto:

- Actuación urgente y control judicial:
 - o En situaciones de urgencia y cuando exista un interés constitucional legítimo, la Policía Judicial puede realizar un examen directo de los datos contenidos en un dispositivo incautado.
 - o Esta actuación debe ser notificada de inmediato, y en un plazo máximo de 24 horas, al juez competente, mediante un informe escrito y motivado.
 - o El informe debe detallar las razones que justificaron la medida, las acciones llevadas a cabo, la forma en que se realizó el examen y los resultados obtenidos.
 - o El juez, a su vez, tiene un plazo máximo de 72 horas para revocar o confirmar la actuación policial.
- Protección de los derechos del titular de los datos:
 - o El apartado 2 del artículo establece una salvaguarda para evitar el incautamiento de soportes físicos que contengan datos informáticos, siempre que sea posible obtener una copia de los mismos.
 - o Esta medida busca proteger al titular de los datos de perjuicios graves, a menos que los soportes sean objeto o instrumento del delito, o existan otras razones que justifiquen su incautación.
 - o Se prioriza obtener una copia de los datos, siempre que se garanticen la autenticidad e integridad de los mismos.

En resumen, se expone y realza la necesidad de una actuación policial rápida en casos urgentes con la protección de los derechos individuales, estableciendo un control judicial estricto y limitando la intervención de dispositivos móviles cuando sea posible obtener una copia de los datos almacenados en los mismos.

Recordemos que el bien jurídico protegido en este tipo de delitos es la intimidad, que es un derecho fundamental reconocido en el artículo 18 de la CE y cuando se realizan estas grabaciones ilegales, existe un apoderamiento del infractor para descubrir los secretos (artículo 197.1 del Código Penal) o atentar contra la intimidad personal de los agentes. Asimismo, esta es la vía menos idónea, no obstante, existe esta opción en el ordenamiento jurídico-penal y la podemos usar llegado el caso.

La misión y objetivo principal es proteger la intimidad, derecho fundamental estrictamente protegido en el artículo 18 de la CE en el que se garantizan los derechos fundamentales al honor, a la intimidad de las personas en su ámbito más privado y al disfrute de su imagen sin interferencia de otros. Este derecho se divide en dos conceptos; por una parte, la intimidad corporal, y por la otra, la intimidad personal.

La intimidad personal se relaciona de forma directa con la libertad del individuo, es decir, con las aptitudes positivas de intervención para gestionar la información respecto a su persona y su familia en su dimensión pública. La noción de secreto, por otra parte, puede definirse como conocimientos que solo son accesibles a unas pocas personas, que deben estar, en última instancia, conectados a la intimidad, dado que esa es la finalidad protectora del tipo. En este sentido, la sentencia 666/2006, Tribunal Supremo, Sala de lo Penal, Sección 1, Rec. 1392/2005 de 19 de junio de 2006, afirma que la sola idea de secreto (artículo 197.1 CP) está estrechamente unida con la intimidad de las personas que se define como el más estricto ámbito privado y de reserva que le protege de la acción del conocimiento de los otros. Estos preceptos son recogidos de forma precisa en el título dedicado a la protección de estos derechos (contra la intimidad), y está estrechamente vinculado con su propia inclusión en el mismo, ya que en el primer apartado se relaciona los papeles, cartas o mensajes de correo electrónico con otros documentos o efectos personales y en la segunda opción destacan los datos que están reservados y son de carácter familiar y/o personal.

7. CONCLUSIONES.

Con referencia a lo anteriormente reseñado, se expone y propone a continuación un cuadro- resumen de las posibles infracciones que cometen las personas cuando graban con sus teléfonos móviles las actuaciones de la Policía, y no precisamente por tener un derecho legítimo a la información, sino por intentar desprestigiar, menospreciar y faltar al respeto a los agentes actuantes.

CUADRO DE INFRACCIONES A DIFERENTES NORMAS.			
ARTÍCULO	NORMA.	CONCEPTO.	REQUISITOS.
36.23, infracción grave.	LOPSC.	Usar las imágenes o datos de origen personal o profesional de autoridades o miembros de las FF.CC.SS. con peligro para éstos y sus familias, así como el de las instalaciones policiales o actuaciones policiales de importancia. <u>Sanción:</u> De 601 a 30.000 €.	<u>Es necesario:</u> 1º. Identificar al infractor e informarle del motivo. 2º. Que posteriormente, el infractor “cuelgue” en Facebook o Whatsapp las imágenes de la intervención.
			3º. Que dichas imágenes supongan un peligro para los agentes o sus familias.
			4º. Grabación en soporte DVD, CD, o pendrive de las imágenes para el envío al órgano instructor.
			Puede pasar, como ya ha pasado, que, a pesar de distribuir las imágenes de la actuación policial, el instructor¹ del procedimiento establezca que no hay peligro para los agentes y se ARCHIVE la denuncia.
37.4, infracción leve.	LOPSC.	Las faltas de respeto y consideración debida a los agentes de las FF.CC.SS. cuando se encuentren realizando sus funciones y que estas conductas no sean catalogadas o tipificadas como delito	En muchísimos casos estos infractores FALTAN AL RESPETO de los agentes desde el primer momento, ya que interfieren, desprecian y menoscaban la actuación de los agentes.

		(556 CP). <u>Sanción:</u> De 100 a 600 €.	
No es únicamente esto lo que se debe considerar al fotografiar o grabar a los agentes de policía. Y es que, a pesar de que el simple tratamiento de datos personales de los policías, como puede ser la toma de una fotografía o captura de video de ellos, no constituye una infracción de la seguridad ciudadana protegida por la ley. Ello puede dar lugar a otro tipo de infracción administrativa; esto es lo que ha evidenciado la Agencia Española de Protección de Datos en dos de sus resoluciones del año 2018: la Resolución 778 y la 938.			
72.1.b), infracción muy grave.	LOPD.	El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679 (consentimiento del interesado). <u>Sanción:</u> Superior a 300.000 €. Es evidente que no se impondrá esta sanción, pero así está catalogada en la LOPD.	Cuando el infractor es requerido e informado por los agentes sobre estos derechos y que <u>no tiene su consentimiento</u>. Se procede a la identificación y si, en el futuro, publica los datos de dicha grabación puede ser denunciado por estos hechos. Hay que enviar una copia de la grabación (DVD, CD, pendrive) así como el informe de los hechos, a la Agencia Española de Protección de Datos², para que inicie el procedimiento sancionador.
73.c), infracción grave.	LOPD.	Impedir u obstaculizar o no atender a los derechos de acceso, de rectificación, supresión o limitación en el tratamiento de los datos. <u>Sanción:</u> De 40.001 a 300.000 €.	Igual al anterior, con la diferencia que se trata de una infracción grave.

74.a), infracción	LOPD.	Incumplir con el principio de transparencia de los datos almacenados	Igual al anterior, con el matiz de que esta infracción es de
------------------------------	-------	--	--

Como recomendación sería mejor la denuncia a la LOPD, ya que, aún en el caso de que se grabe la imagen de los policías y que se publique en las redes sociales, puede dar lugar al archivo de las actuaciones porque al órgano instructor le parezca que no hay peligro para los agentes o sus familiares. Además, la sanción es mucho más elevada. Por ello, aunque se tenga que enviar todo el expediente (acta de denuncia o informe y la grabación de las imágenes publicadas en soporte DVD, CD o pendrive) a la dirección en Madrid de la Agencia Española de Protección de Datos, es más que aconsejable hacerlo con el objeto de que este tipo de infractores sean sancionados debidamente. Como ejemplo de expedientes sancionadores:

1. Procedimiento número PS/00576/2017, resolución número R/00778/2018, de la Agencia Española de Protección de Datos, multa de 2.000 € (grabación de policías locales y publicado en Whatsapp).
2. Procedimiento número PS/00046/2018, resolución número R/00938/2018, de la Agencia Española de Protección de Datos, multa de 1.500 € (grabación de guardias civiles y publicado en Facebook).

En base al informe jurídico de la AEPD número 77 del año 2013, en el que se establece la exclusión de la aplicación de la LOPD, cuando se den los siguientes casos:

- **Exclusión de la LOPD en actividades personales o domésticas:**

o No se aplica al tratamiento de datos realizado por cualquier persona en sus actividades y quehaceres personales o domésticos (grabaciones de la vida privada de las personas).

- **Límites de la excepción:**

o Sin embargo, la AEPD aclara que esta excepción se limita a actividades que se inscriben en el marco de la vida privada o familiar.

o No se aplica a fotografías o videos de funcionarios públicos durante el ejercicio de sus funciones.

- **Difusión en internet:**

o La difusión de estas imágenes o videos en internet, haciéndolos accesibles a un grupo indeterminado de personas, queda fuera del ámbito de las actividades personales o domésticas.

o Esta interpretación se basa en la Sentencia del Pleno del Tribunal de Justicia de las Comunidades Europeas de 6 de noviembre de 2003.

- **Implicaciones:**

o En resumen, grabar a un funcionario público en su vida privada, puede entrar dentro del amparo de la vida privada, pero grabarles en el ejercicio de sus funciones, y más aun difundirlo por internet, sale de ese amparo, y se puede entrar en conflictos legales al vulnerar la legislación sobre la protección de datos personales.

Para finalizar, tras realizar una consulta a la AEPD sobre la procedencia de la intervención del teléfono móvil u otro artefacto ante este tipo de grabaciones durante las actuaciones policiales, sin el consentimiento de los policías, y con la negativa a parar de grabar ni respetar los derechos de acceso, rectificación, cancelación y oposición (ARCO) por parte de los infractores, y a los efectos de realizar la correspondiente denuncia a la LOPD (LO 3/2018, de 5 de diciembre) la AEPD contestó lo siguiente:

Se podrá interponer una denuncia ante la Agencia cuando las imágenes que se han tomado se difunden en abierto y esa difusión supone una infracción a la LOPD, es decir, en relación con al uso y finalidad que se realiza posteriormente con las imágenes, lo que NO implica la intervención de los teléfonos y es lo que habría que demostrar sin perjuicio de otros derechos como serían la libertad de expresión e información o el derecho a la tutela judicial, como dispone el considerando número 4 del Reglamento de la UE relativo a la protección de las personas físicas en lo concerniente al tratamiento de los datos personales.

El Considerando 4 del Reglamento Europeo que regula la protección de los datos personales de las personas resalta la importancia de tratar los datos personales de manera que beneficien a la humanidad. Es fundamental entender que, aunque tenemos el derecho a la protección de nuestros datos, este derecho no es absoluto. Debe equilibrarse con otros derechos fundamentales, siguiendo el principio de proporcionalidad. Esto significa que, en ciertas situaciones, puede ser necesario priorizar otros derechos o intereses sociales.

Además, el reglamento mencionado se asegura de que se respeten todos los derechos fundamentales, como la privacidad, la libertad de expresión y el derecho a un juicio justo, entre otros. En resumen, se trata de encontrar un balance que permita proteger nuestros datos personales mientras se promueven otros valores esenciales en la sociedad.

8. BIBLIOGRAFÍA Y WEBGRAFÍA.

- Constitución Española de 1978.
- Código Penal, LO 10/1995, de 23 de noviembre.
- Ley orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y a la propia imagen.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

- Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana.
- Resoluciones de la AEPD números R/00778/2018 y R/00938/2018.
- Informe jurídico de la AEPD número 0077/2013.
- Nota informativa del Tribunal Constitucional número 108/2020.
- Instrucción de la Secretaría de Estado de Seguridad número 13/2018, de 17 de octubre.
- Sentencia de la Audiencia Provincial de Burgos número 113/2006, de 31 de marzo.
- Sentencia de la Audiencia Provincial de Madrid número 120/2008, de 11 de marzo.
- <https://www.debelareabogados.es/>.
- <https://guiasjuridicas.wolterskluwer.es/>.

Noticias

SIP-AN REQUIERE EL CESE INMEDIATO DEL USO DE SU NOMBRE CON FINES COMERCIALES**08-07-2026**

Desde hace meses que venimos recibiendo quejas de ciudadanos que son contactados por una actividad de telemarketing orientada a la comercialización telefónica de inserciones y espacios publicitarios para su pretendida publicación en una revista a cambio de una prestación económica.

SIP-AN no tiene relación comercial alguna con ninguna empresa para este fin, por lo que se **DESLIGA Y SEPARA ABSOLUTAMENTE** de toda actuación que requiera un requerimiento económico.

Hemos puesto en manos de nuestros servicios jurídicos la situación, requiriendo a la empresa, ACTIVIDAD DE COBROS PUBLICITARIOS S.L que, de forma terminante CESE TOTAL Y DEFINITIVO de toda comunicación en la que sus comerciales, agentes, teleoperadores o filiales invoquen o usen nuestra denominación, iniciales, acrónimo o cualquier combinación que induzca a confusión de identidad.

No vamos a permitir que nuestro nombre sea usado de forma que se abuse de la buena fe y predisposición de los ciudadanos, con la consiguiente usurpación de identidad y el daño reputacional y de imagen de nuestro sindicato.

<https://ayuntamientoboadilladelmonte.org/boadilla-actualidad/noticias/la-policia-local-alerta-de-varios-intentos-de-estafa-comercios-con-una>

https://www.malagahoy.es/marbella/suplantan-policia-local-marbella-estafas-0-2007297217.html?utm_source=malagahoy&utm_medium=push&utm_campaign=17.00_suplantan

<https://www.pontevedraviva.com/es/general/estafadores-piden-en-marin-dinero-en-publicidad-para-una-falsa-revista-policia-324107-102.html>



SIP-AN DENUNCIA EL GRAVE DETERIORO DEL SERVICIO DE LA POLICÍA LOCAL DE BAEZA Y ADVIERTE DEL RIESGO PARA LA SEGURIDAD CIUDADANA

14-07-2026

El Sindicato Independiente de Policía de Andalucía (SIP-AN) ha denunciado públicamente la preocupante situación que atraviesa la Policía Local de Baeza, tras varios días en los que, según el sindicato, el servicio se ha prestado con una dotación de agentes claramente insuficiente para garantizar la seguridad de la ciudadanía y de los propios policías.

Desde la sección sindical de SIP-AN en Baeza se atribuye esta situación a la falta de diálogo con la plantilla y a la ausencia de medidas por parte del equipo de gobierno municipal para resolver el conflicto existente, lo que estaría provocando una progresiva merma del servicio policial.

Plantillas bajo mínimos

Según denuncia el sindicato, durante el pasado fin de semana la ciudad contó únicamente con un agente en el turno de mañana, ningún policía en el turno de tarde y dos agentes durante la noche, una dotación que consideran insuficiente para atender con garantías las necesidades de una población como Baeza.

Además, la situación habría continuado durante el lunes 13 de julio, con un solo agente de radiopatrulla por la mañana y ausencia de patrullas en el turno de tarde, circunstancia que, según SIP-AN, evidencia que no se trata de un hecho aislado sino de un problema estructural.

Como consecuencia, el sindicato asegura que numerosos avisos y requerimientos vecinales no pudieron atenderse o sufrieron importantes retrasos debido a la escasez de efectivos disponibles.

Preocupación por la seguridad de las dependencias policiales

SIP-AN también muestra su preocupación por los periodos en los que las dependencias policiales permanecen sin presencia de agentes, advirtiendo del riesgo que ello supone para la custodia de documentación, armamento y demás material policial.

El sindicato recuerda que recientemente se han conocido intentos de robo de material policial en otras jefaturas, por lo que considera imprescindible mantener las instalaciones debidamente protegidas.

Falta de presencia policial durante los exámenes de acceso a la Guardia Civil

Entre los hechos denunciados destaca igualmente el dispositivo desarrollado con motivo de los exámenes de acceso a la Guardia Civil celebrados el pasado 11 de julio en Baeza.

Según SIP-AN, más de 3.000 aspirantes y familiares se desplazaron hasta la localidad sin que existiera presencia de patrullas de Policía Local regulando el tráfico en los accesos a

la Academia, lo que habría provocado importantes retenciones y situaciones de riesgo para conductores y peatones en una jornada de gran afluencia.



Críticas por la celebración de la procesión de San Cristóbal

Otro de los episodios denunciados hace referencia a la procesión de San Cristóbal celebrada ese mismo fin de semana.

El sindicato afirma que el Jefe de la Policía Local emitió un informe advirtiendo de que no existían efectivos suficientes para garantizar la seguridad del evento y proponiendo su suspensión. Sin embargo, sostiene que el Ayuntamiento autorizó finalmente su celebración.

Asimismo, SIP-AN denuncia que durante el desarrollo del acto participaron vigilantes de seguridad privada, personal auxiliar y voluntarios de Protección Civil realizando funciones relacionadas con la regulación del tráfico, actuaciones que, a juicio del sindicato, podrían invadir competencias reservadas legalmente a las Fuerzas y Cuerpos de Seguridad.

Por este motivo, la organización sindical ha anunciado que solicitará al Ayuntamiento toda la documentación relativa al dispositivo de seguridad para su análisis por parte de los servicios jurídicos del sindicato, con el fin de valorar el ejercicio de las acciones legales que pudieran corresponder.

SIP-AN reclama soluciones urgentes

Desde SIP-AN lamentan que la falta de efectivos continúe deteriorando la calidad del servicio que reciben los vecinos de Baeza y reiteran que la seguridad ciudadana debe situarse por encima de cualquier conflicto laboral o político.

El sindicato asegura mantener abierta la vía del diálogo con la corporación municipal, aunque advierte de que, si no se adoptan medidas para reforzar la plantilla y resolver el conflicto existente, intensificará su acción sindical en defensa tanto de los profesionales de la Policía Local como de la seguridad de la ciudadanía.

DOS NUEVAS SENTENCIAS DEL TSJA DAN LA RAZÓN A SIP-AN Y CONSOLIDAN EL DERECHO DE LA POLICÍA LOCAL A COBRAR LOS PLUSES DURANTE VACACIONES, PAGAS EXTRA E IT

20-07-2026

El Sindicato Independiente de Policía de Andalucía (SIP-AN) continúa obteniendo importantes avances en la defensa de los derechos económicos de sus afiliados. El Tribunal Superior de Justicia de Andalucía (Sala de Málaga), mediante las sentencias nº 1345/2026 y 1348/2026, ha desestimado los recursos de apelación interpuestos por el Ayuntamiento de Benalmádena y ha confirmado íntegramente las resoluciones favorables obtenidas por los servicios jurídicos del sindicato.

Estas resoluciones suponen un nuevo respaldo a la labor desarrollada por SIP-AN y consolidan una doctrina de enorme trascendencia para los policías locales que prestan servicio en régimen de turnos.

Los pluses forman parte de la retribución ordinaria

El TSJA reconoce que los agentes tienen derecho a seguir percibiendo durante sus vacaciones los complementos correspondientes a:

Nocturnidad.

Servicios prestados en sábados.

Servicios prestados en domingos.

Servicios prestados en días festivos.

La Sala considera que estas cantidades no constituyen gratificaciones por servicios extraordinarios, sino que forman parte de la retribución complementaria ordinaria al estar directamente vinculadas a las condiciones habituales de prestación del servicio.

Como consecuencia, dichos conceptos deben abonarse igualmente durante el período vacacional e integrarse en las pagas extraordinarias.

Una doctrina respaldada por el Tribunal Supremo

Las sentencias aplican la doctrina ya consolidada por el Tribunal Supremo, especialmente la contenida en las sentencias de 1 de octubre de 2020 y 4 de julio de 2024, reforzando así la seguridad jurídica de los policías locales.

Además, el Tribunal extiende este criterio a las situaciones de incapacidad temporal y demás permisos retribuidos, entendiendo que cuando la nocturnidad y los festivos forman parte de la jornada ordinaria de trabajo, su percepción no puede verse interrumpida por el disfrute de vacaciones o por una baja médica.

El TSJA rechaza los argumentos del Ayuntamiento

El Ayuntamiento de Benalmádena sostenía que estos complementos carecían de una configuración jurídica independiente y que su abono supondría una duplicidad con el complemento específico.

Sin embargo, el Tribunal rechaza íntegramente dichos argumentos y confirma la corrección de la interpretación jurídica defendida por SIP-AN desde el inicio del procedimiento.

Condena en costas al Ayuntamiento

Las dos resoluciones imponen además las costas procesales de la apelación al Ayuntamiento de Benalmádena, fijando un límite máximo de 1.000 euros por cada procedimiento, al haber sido desestimados íntegramente sus recursos.

Esta condena evidencia la solidez de la posición jurídica mantenida por el sindicato y la falta de fundamento de la impugnación municipal.

Un nuevo éxito jurídico de SIP-AN

Con estas dos nuevas sentencias, SIP-AN sigue consolidando una línea jurisprudencial que protege los derechos retributivos de los policías locales andaluces.

Este importante pronunciamiento garantiza que los complementos derivados del trabajo a turnos formen parte de la retribución ordinaria, evitando que los agentes sufran pérdidas económicas durante sus vacaciones, las pagas extraordinarias, las situaciones de incapacidad temporal o cualquier otro permiso retribuido.

Desde SIP-AN continuaremos defendiendo, por todas las vías legales, los derechos laborales y económicos de nuestros afiliados, demostrando una vez más que el trabajo jurídico riguroso y la acción sindical eficaz ofrecen resultados reales para la Policía Local de Andalucía.



NUEVA SENTENCIA CONDENATORIA OBLIGA AL AYUNTAMIENTO DE SAN FERNANDO A INDEMNIZAR A UN AGENTE DE POLICÍA LOCAL LESIONADO EN ACTO DE SERVICIO**30-07-2026**

LA JUSTICIA ESTIMA ÍNTEGRAMENTE LA RECLAMACIÓN PROMOVIDA TRAS LA INSOLVENCIA DEL AGRESOR Y REAFIRMA EL PRINCIPIO DE INDEMNIDAD QUE PROTEGE A LOS AGENTES EN EL EJERCICIO DE SUS FUNCIONES

La Sentencia n.º 155/2026, dictada el 20 de julio de 2026 por el Juzgado de lo Contencioso-Administrativo n.º 2 de Cádiz, ha estimado íntegramente el recurso interpuesto por un agente de la Policía Local de San Fernando frente al silencio administrativo del Ayuntamiento ante su reclamación de responsabilidad patrimonial subsidiaria.

El procedimiento tiene su origen en las lesiones sufridas por el agente durante una intervención policial en acto de servicio. Dichos hechos dieron lugar a un procedimiento penal que concluyó con la condena del agresor. Sin embargo, tras ser declarado insolvente, la indemnización reconocida judicialmente quedó sin abonar.

Pese a la consolidada doctrina del Tribunal Supremo sobre el principio de indemnidad, que garantiza que los empleados públicos sean resarcidos por los daños sufridos en el ejercicio de sus funciones cuando no exista culpa o negligencia por su parte, el Ayuntamiento de San Fernando rechazó asumir el pago de la indemnización. Esta negativa obligó a acudir nuevamente a los tribunales para hacer valer los derechos del agente.

La sentencia condena al Ayuntamiento de San Fernando a abonar la indemnización correspondiente, junto con los intereses legales devengados, e impone además el pago de las costas procesales al estimar íntegramente la demanda. La resolución es firme y no cabe recurso contra la misma.

Este nuevo pronunciamiento judicial constituye un importante respaldo a la protección jurídica de los agentes y reafirma la obligación de las Administraciones Públicas de responder cuando un agente resulta lesionado en acto de servicio y el responsable de los hechos es insolvente.

Desde SIP-AN queremos trasladar nuestra más sincera enhorabuena al compañero por la defensa de sus derechos, así como felicitar a la Sección Sindical de San Fernando por el trabajo y la confianza depositada durante todo el procedimiento.

Asimismo, expresamos nuestro reconocimiento al despacho de abogados de Alberto Prián, cuya excelente dirección jurídica ha sido determinante para la obtención de este nuevo éxito judicial.

En SIP-AN seguimos siempre al lado de nuestros compañeros, defendiendo sus derechos e intereses con firmeza y compromiso.

SIP-AN SUPERA LOS 2.500 AFILIADOS Y CONTINÚA AFIANZÁNDOSE COMO EL SINDICATO MAYORITARIO DE POLICÍA LOCAL EN ANDALUCÍA**04-08-2026**

EL GRACIAS AL RESPALDO DE MILES DE POLICÍAS LOCALES, EL SINDICATO SIGUE CRECIENDO EN DEFENSA DEL COLECTIVO

Desde SIP-AN tenemos el orgullo de anunciar que ya somos más de 2.500 afiliados repartidos por toda Andalucía. Un crecimiento que nos consolida como el sindicato mayoritario de Policía Local en Andalucía y que nos impulsa a seguir trabajando con más fuerza, más responsabilidad y el mismo compromiso que nos ha acompañado desde el primer día.

Este importante hito no sería posible sin la confianza de cada uno de los compañeros y compañeras que han decidido formar parte de este proyecto. A todos vosotros, gracias. Gracias por creer en una forma diferente de hacer sindicalismo, por confiar en nuestro trabajo y por demostrar que la unión de los Policías Locales es la mejor herramienta para defender nuestros derechos.

Hoy, SIP-AN cuenta con 82 secciones sindicales distribuidas por numerosos municipios andaluces, una implantación que continúa creciendo y ampliándose gracias al esfuerzo diario de nuestros delegados y afiliados. Esta presencia nos permite estar cerca de los compañeros, conocer de primera mano sus necesidades y defender sus intereses allí donde sea necesario.

Nuestro crecimiento no responde a una casualidad. Es el resultado de un trabajo constante, de una organización cercana y de una forma de entender el sindicalismo basada exclusivamente en la defensa de la Policía Local. Somos un sindicato profesional e independiente de cualquier ideología política, cuyo único objetivo es proteger los derechos, los intereses profesionales y las condiciones laborales de todos los Policías Locales de Andalucía.

Cada nueva afiliación representa mucho más que un número. Es una muestra de confianza, un respaldo al trabajo realizado y un compromiso compartido con la mejora de nuestra profesión. Nos anima a seguir reivindicando una Policía Local más reconocida, mejor protegida y con las condiciones laborales que merece.

SIP-AN no es solo un sindicato. Es el resultado de la unión, la determinación y el compromiso de miles de Policías Locales que creen en un sindicalismo profesional, independiente y verdaderamente al servicio de quienes visten cada día el uniforme.

Desde SIP-AN queremos reiterar nuestro más sincero agradecimiento a todos los afiliados, delegados y compañeros que forman parte de esta gran familia. Este logro pertenece a todos vosotros. Seguiremos trabajando con la misma cercanía, transparencia y firmeza que nos han traído hasta aquí, porque aún quedan muchos retos por alcanzar y estamos convencidos de que, unidos, seguiremos haciendo crecer la voz de la Policía Local en toda Andalucía.

Gracias por vuestra confianza. Gracias por formar parte de SIP-AN.



Descuentos

CASALEIZ PSICOLOGÍA

CONVENIO DE COLABORACIÓN

En Casaleiz Psicología somos especialistas en Terapias de Tercera Generación, especializándonos en:

Terapia de pareja

Ansiedad

Dependencia Emocional

Mediación Familiar

Fobias

Gestión Emocional

- Psicoterapia individual. Precio Afiliado 50€
- Psicoterapia de pareja. Precio Afiliado 55€



Casaleiz
PSICOLOGÍA

MIRANZA (OFTALMOLOGÍA)

CONVENIO DE COLABORACIÓN

Nuevo descuento para afiliados a SIP-AN y familiares directos siempre que se acredite en la primera visita.

- 15% de descuento en revisiones y pruebas diagnósticas.
- 10% de descuento en cirugías y otros tratamientos.

MIRANZA



Tu visión en las mejores manos

15% de descuento en primera consulta y pruebas diagnósticas y **10% de descuento** en cirugías y otros tratamientos. Descuentos aplicables únicamente sobre la tarifa privada.

Accede a la web de miranza para reservar cita en tu clínica más cercana

Miranza, grupo líder en oftalmología, con más de 35 centros en España, cuenta con oftalmólogos de gran prestigio y con la última tecnología al servicio de la visión.

¡Aprovecha esta oportunidad y pon a punto tu visión!

CATARATAS • PRESBICIA • CIRUGÍA REFRACTIVA • RETINA • Córnea • OJO SECO • GLAUCOMA
OFTALMOLOGÍA PEDIÁTRICA • ESTRABISMO DEL ADULTO • OCULOPLÁSTICA • ESTÉTICA OCULOFACIAL

Válido hasta Septiembre, 2027
Promoción no acumulable a otras ofertas
Imprescindible presentar acreditación de colectivo

www.miranza.es

PARQUES REUNIDOS**CONVENIO DE COLABORACIÓN**

Disponibles ventajosos descuentos en diferentes parques para afiliados a SIP-AN y un máximo de 3 acompañantes.

➡ Puedes solicitarnos tu código de descuento en el email de contacta@sip-an.es indicándonos tu nombre, apellidos y DNI y el nombre del parque para el que necesitas el código

Descuentos especiales en Zoo, Atlantis, Parque de Atracciones de Madrid, Faunia y Parque Warner

- Sirven para entradas de adulto y niño / senior. A todos ellos se les aplica el mismo precio. No aplican a otros tipos de entradas (2º día, discapacitados...) ni servicios (parking de pago, menús, fast pass...), ni son acumulables a otras promociones.
- Cada código permite comprar hasta 4 entradas en total.
- Deben usarse, al menos, con un día de antelación (no para el mismo día de la visita).
- Son válidos hasta 31-01-2027, según días oficiales de apertura de cada parque.
 - No aplican para visitas los días 31 de octubre y 1 de noviembre de 2026 en Parque Warner Madrid y Parque de Atracciones de Madrid.
 - Los precios indicados son unitarios, incluyen IVA y pueden ser modificados por los parques en cualquier momento sin previo aviso.
 - Consultar calendario, horarios de apertura y normas de cada parque en su web oficial.

+ Otros parques y precios:

- Parque Warner Beach: 21,90 € (temporada desde 6 de junio hasta 6 de septiembre de 2026).
- Aquopolis Villanueva: 22,90 € (temporada desde 12 de junio hasta 6 de septiembre de 2026).
- Aquopolis Costa Dorada: 22,95 € (temporada desde 1 de junio hasta 13 de septiembre de 2026).
- Aquopolis Torrevieja: 23,95 € (temporada desde 8 de junio hasta 6 de septiembre de 2026).
- Aquopolis Cullera: 22,95 € (temporada desde 15 de junio hasta 6 de septiembre de 2026).
- Aquopolis Cartaya: 19,90 € (temporada desde 1 de julio hasta 6 de septiembre de 2026).



Parques Reunidos
PASSION
FOR LEISURE



PARQUE DE
ATRACCIONES
MADRID

24,90€



ZOO
AQUARIUM
MADRID

20,50€



PARQUE W
B WARNER
MADRID

34,90€



FAUNIA

19,90€



ATLANTIS
AQUARIUM

11,90€

