Dirección Adjunta Operativa (DAO)

El **Real Decreto 952/2018, de 27 de julio**, desarrolla la estructura orgánica básica del Ministerio del Interior. En el ámbito de la **Dirección General de la Policía** se ha considerado conveniente, en beneficio de una mejor coordinación de las distintas Unidades operativas, recuperar la figura de la Dirección Adjunta Operativa. El Ministro del Interior ha nombrado Director Adjunto Operativo de la Policía Nacional al Comisario Principal **José Ángel González Jiménez.**

La **Dirección Adjunta Operativa (DAO)** es la encargada de la colaboración con el Director General de la Policía en la dirección de las funciones de mantenimiento del orden y la seguridad ciudadana; la dirección, coordinación y supervisión de las Unidades centrales, supraterritoriales y territoriales, el seguimiento y control de los resultados de los programas operativos, y en la definición de los recursos humanos y materiales aplicables a dichos programas; y la Oficina Central Nacional de INTERPOL, la Unidad Nacional de EUROPOL y la Oficina SIRENE.

La **DAO** es responsable, de acuerdo con las directrices emanadas del Director General, de la dirección, impulso y coordinación de las funciones policiales operativas, que en el nivel central serán realizadas por las comisarías Generales de Información de Policía Judicial, de Seguridad Ciudadana, de Extranjería y Fronteras y de Policía Científica, todas ellas con nivel orgánico de subdirección general, correspondiéndoles:

a) A la **Comisaría General de Información (CGI)**, la captación, recepción, tratamiento y desarrollo de la información de interés para el orden y la seguridad pública en el ámbito de las funciones de la Dirección General, así como su explotación o aprovechamiento operativo, especialmente en materia antiterrorista, tanto en el ámbito nacional como en el internacional.
b) A la **Comisaría General de Policía Judicial (CGPJ)**, la investigación y persecución de las infracciones supraterritoriales, especialmente de los delitos relacionados con las drogas, la delincuencia organizada, económica, financiera, tecnológica y el control de los juegos de azar. Asimismo, le corresponde la dirección de los servicios encargados de la investigación de delitos monetarios y los relacionados con la moneda, así como la colaboración con los servicios correspondientes del Banco de España en estos asuntos.
c) A la **Comisaría General de Seguridad Ciudadana (CGSC)**, la organización y gestión de lo relativo a la prevención, mantenimiento y, en su caso, restablecimiento del orden y la seguridad ciudadana; **las competencias que le encomienda la legislación sobre Seguridad Privada**; la vigilancia de los espectáculos públicos, dentro del ámbito de competencia del Estado, y la protección de altas personalidades, edificios e instalaciones que por su interés lo requieran.
d) A la **Comisaría General de Extranjería y Fronteras (CGEYF)**, el control de entrada y salida del territorio nacional de españoles y extranjeros; la prevención, persecución e investigación de las redes de inmigración ilegal, y, en general, el régimen policial de extranjería, refugio y asilo e inmigración.
e) A la **Comisaría General de Policía Científica (CGPC)**, la prestación de los servicios de criminalística, identificación, analítica e investigación técnica, así como la elaboración de los informes periciales y documentales que le sean encomendados.

UNIDAD CENTRAL DE SEGURIDAD PRIVADA
R@S - Telf.: **913223951 -** Email: **redazul@policia.es**

ÍNDICE:

1. Estructura periférica de Seguridad Privada de la Policía Nacional.
2. Videovigilancia: la gestión de las imágenes.
3. La protección de datos de carácter personal.
4. Planes de Apoyo Operativo en Infraestructuras Críticas.
5. El síndrome de estrés postvacacional.
6. Informe Técnico: Diseño de un Curso de introducción a las TIC corporativas.
7. Formación: Jornadas formativas de prevención antiterrorista e Interlocutor Policial Sanitario en diferentes localidades españolas.

1. Estructura periférica de Seguridad Privada.

La **Seguridad Privada de la Policía Nacional** en su ámbito periférico está formada por **Unidades Territoriales**, incardinadas en el área de seguridad ciudadana y coordinadas por la Unidad Central de Seguridad Privada, constituyendo el canal profesional previamente predeterminado que ha de ser utilizado por la Policía Nacional y el Sector de la Seguridad Privada para establecer las relaciones de colaboración en su ámbito territorial.

Con la finalidad de mejorar la coordinación y evitar posibles disfunciones, los requerimientos de información que se consideren necesarios para la práctica de actuaciones operativas, tanto los procedentes de la Policía Nacional como del Sector de la Seguridad Privada, se realizarán a través de las respectivas Unidades Territoriales, que serán las encargadas de canalizar la información generada por el Sector, para que pueda ser debidamente evaluada, y de establecer el contacto profesional que resulte necesario en cada caso.

Las Unidades Territoriales, además de los cometidos propios de control e inspección de la Seguridad Privada establecidos reglamentariamente, tienen la misión de actuar como canal de trasmisión entre la Policía Nacional y los distintos organismos y entidades del Sector de la Seguridad Privada, llevando a cabo las siguientes actuaciones:

- Canalizar los respectivos requerimientos de colaboración que se dirijan entre las Unidades Policiales de la Policía Nacional Policía y el Sector de la Seguridad Privada, recibiendo y facilitando las respuestas a los requerimientos efectuados.
- Facilitar el contacto y el conocimiento, institucional y operativo, entre las distintas Unidades de la Policía Nacional y las entidades, responsables y usuarios del Sector de la Seguridad Privada.
- Coordinar y difundir la información operativa que se produzca en el Sector de la Seguridad Privada o que pueda ser de su interés.

Los requerimientos de información se realizarán cumplimentando los respectivos formularios, que serán remitidos a través de la Unidad Territorial de Seguridad Privada correspondiente, que será quien mantenga el contacto con el destinatario, al que enviará el requerimiento y recibirá de él la respuesta adecuada, que a su vez hará llegar al requirente.

Todo lo anterior, sin perjuicio del contacto directo que pueda establecerse con la Unidad Policial concernida para el mejor seguimiento del asunto, aclaración de dudas o aquellas cuestiones que se consideren de interés por las partes.

UNIDADES TERRITORIALES DE POLICÍA NACIONAL

ALBACETE
Dirección: c/ Dionisio Guardiola, nº 27
Teléfono: 967503045
Email: albacete.segpriv@policia.es

ÁVILA
Dirección: c/ Dionisio del Embarcadero, s/n
Teléfono: 920353966
Email: avila.segpriv@policia.es

ALGECIRAS
Dirección: Avda. del Embarcadero, s/n
Teléfono: 956588437
Email: algeciras.segpriv@policia.es

BADAJOZ
Dirección: Avda. Cuerpo Nacional de Policía, s/n
Teléfono: 924207100
Email: badajoz.segpriv@policia.es

ALMERÍA
Dirección: c/ Alcalde Muñoz, nº 40
Teléfono: 950623137
Email: almeria.segpriv@policia.es

BARCELONA
Dirección: c/ Balmes, nº 192
Teléfono: 932903151
Email: barcelona.segpriv@policia.es

ESTRUCTURA TERRITORIAL SEGURIDAD PRIVADA I

BILBAO
Dirección: Avda. Lendakari Aguirre, nº 90
Teléfono: 944709189
Email: bilbao.segpriv@policia.es

BURGOS
Dirección: Avda. Castilla y León, nº3
Teléfono: 947282319
Email: burgos.segpriv@policia.es

CÁCERES
Dirección: Avda. Pierre Coubertain, nº 13
Teléfono: 927626523
Email: caceres.segpriv@policia.es

CÁDIZ
Dirección: c/ Santa María Soledad, nº 6
Teléfono: 956297535
Email: cadiz.segpriv@policia.es

CASTELLÓN
Dirección: c/ Río Sella, nº 5
Teléfono: 964469539
Email: castellon.segpriv@policia.es

CEUTA
Dirección: Avda. San Juan de Dios, nº 11
Teléfono: 956513418
Email: ceuta.segpriv@policia.es

CIUDAD REAL
Dirección: Ronda de Toledo, nº 27
Teléfono: 926277914
Email: ciudadreal.segpriv@policia.es

CÓRDOBA
Dirección: Avda. Campo Madre de Dios, nº 11
Teléfono: 957594526
Email: cordoba.segpriv@policia.es

CUENCA
Dirección: c/ Luis Astrana Martín, nº 4
Teléfono: 969240798
Email: cuenca.segpriv@policia.es

GERONA
Dirección: c/ Sant Pau, nº 2
Teléfono: 972411553
Email: gerona.segpriv@policia.es

GIJÓN
Dirección: Plaza Padre Máximo González, s/n
Teléfono: 985179302
Email: gijon.segpriv@policia.es

GRANADA
Dirección: c/ La Palmita, nº 1
Teléfono: 958808054
Email: granada.segpriv@policia.es

GUADALAJARA
Dirección: Avda. del Ejército, nº 12
Teléfono: 949248413
Email: guadalajara.segpriv@policia.es

HUELVA
Dirección: Pase de la Glorieta, nº 1
Teléfono: 959541918
Email: huelva.segpriv@policia.es

HUESCA
Dirección: Plaza Luis Buñuel, nº 3
Teléfono: 974238826
Email: huesca.segpriv@policia.es

JAÉN
Dirección: c/ Obispo Estuñiga, nº 9
Teléfono: 953296120
Email: jaen.segpriv@policia.es

LA CORUÑA
Dirección: c/ Médico Devesa Núñez, nº 4
Teléfono: 981166406
Email: acoruna.segpriv@policia.es

LAS PALMAS
Dirección: c/ Luis Doreste Silva, nº 68
Teléfono: 928304846
Email: laspalmas.segpriv@policia.es

LEÓN
Dirección: c/ Villabenavente, nº 6
Teléfono: 987218922
Email: leon.segpriv@policia.es

LÉRIDA
Dirección: c/ L'Ensenyanca, nº 2
Teléfono: 973728539
Email: lerida.segpriv@policia.es

LOGROÑO
Dirección: c/ Serradero,, nº 26
Teléfono: 941272079
Email: logroño.segpriv@policia.es

LUGO
Dirección: c/ Chantada, nº 1
Teléfono: 982265124
Email: lugo.segpriv@policia.es

ESTRUCTURA TERRITORIAL SEGURIDAD PRIVADA II

MADRID
Dirección: c/ Mirador de la Reina, nº 4
Teléfono: 913767669
Email: madrid.segpriv@policia.es

MÁLAGA
Dirección: Plaza Manuel Azaña, nº 3
Teléfono: 952046303
Email: malaga.segpriv@policia.es

MALLORCA
Dirección: Simó Ballester, nº 8
Teléfono: 971225295
Email: mallorca.segpriv@policia.es

MELILLA
Dirección: c/ Actor Tallaví, nº 3
Teléfono: 92696378
Email: melilla.segpriv@policia.es

MURCIA
Dirección: Plaza Ceballos, nº 13
Teléfono: 968355586
Email: murcia.segpriv@policia.es

ORENSE
Dirección: c/ Maestro Vide, nº 2-4
Teléfono: 988391382
Email: ourense.segpriv@policia.es

OVIEDO
Dirección: Avd. Buenavista, s/n
Teléfono: 985967171
Email: oviedo.segpriv@policia.es

PALENCIA
Dirección: c/ Simón Nieto, nº 8
Teléfono: 979167419
Email: palencia.segpriv@policia.es

PAMPLONA
Dirección: c/ Beloso Alto, nº 5
Teléfono: 948299538
Email: pamplona.segpriv@policia.es

PONTEVEDRA
Dirección: c/ Joaquín Costa, nº 17-19
Teléfono: 986868357
Email:pontevedra.segpriv@policia.es

SEVILLA
Dirección: c/ Blas Infante, nº12
Teléfono: 954289723
Email: sevilla.segpriv@policia.es

SORIA
Dirección: c/ Nicolás Rabal, nº 9
Teléfono: 975239334
Email: soria.segpriv@policia.es

TARRAGONA
Dirección: Plaza de Orleans, s/n
Teléfono: 977248656
Email: tarragona.segpriv@policia.es

TENERIFE
Dirección: Avd. Tres de Mayo, nº 32
Teléfono: 922849563
Email: sctenerife.segpriv@policia.es

TERUEL
Dirección: c/ Córdoba, nº 2
Teléfono: 978625019
Email: teruel.segpriv@policia.es

TOLEDO
Dirección: Avd. Portugal, s/n
Teléfono: 925288577
Email: toledo.segpriv@policia.es

VALENCIA
Dirección: c/ Bailén, nº 9
Teléfono: 963419095
Email: velencia.segpriv@policia.es

VALLADOLID
Dirección: c/ Gerona, s/n
Teléfono: 983456716
Email: valladolid.segpriv@policia.es

VIGO
Dirección: c/ Luis Taboada, nº 3
Teléfono: 986820307
Email: vigo.segpriv@policia.es

VITORIA
Dirección: c/ Oñate, s/n
Teléfono: 945209636
Email: vitoria.segpriv@policia.es

ZAMORA
Dirección: Avd. de Requejo, nº 12
Teléfono: 980509294
Email: zamora.segpriv@policia.es

ZARAGOZA
Dirección: c/ General Mayandía, nº 3
Teléfono: 976469925
Email:zaragoza.segpriv@policia.es

2. Videovigilancia: la gestión de las imágenes

La videogilancia tiene su regulación en un variado marco normativo:

a) La Constitución Española (Art. 17.1, 18.4 y 104.1)
b) Ley Orgánica 4/1997, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos (Art. 6.1 y Disposición Adicional 9ª).
c) Ley Orgánica 15/1999 de protección de datos de carácter personal (Art. 1 y 2)(LOPD).
d) Instrucción 1/2006 de la Agencia Española de Protección de Datos (Texto expositivo y art. 4).
e) Ley Orgánica 4/2015, de protección de la seguridad ciudadana (Art. 26).
f) Ley 19/2007, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte (Art. 8 y 12.1).
g) Ley 5/2014 de Seguridad Privada (Art. 42).
h) R.D. 2364/1994, Reglamento de Seguridad Privada.
i) Orden INT/314/2011, de empresas de seguridad.
j) Orden INT/316/2011, de alarmas.
k) Orden INT/317/2011, de medidas de seguridad.
l) Orden INT/318/2011, sobre personal de seguridad privada.

La Ley 5/14 de Seguridad Privada (LSP) regula por primera vez en una norma de rango legal y de forma armónica las medidas de seguridad, dotando de concreción a importantes servicios para los que su antecesora, la Ley 23/1992, de 30 de julio, y su reglamento de desarrollo, no contenían regulación alguna, como sucede con la videovigilancia en el ámbito de la seguridad privada, en cumplimiento del mandato contenido en la Ley Orgánica 4/1997, de 4 de agosto, de utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

En el título IV resulta especialmente relevante la regulación de los servicios de videovigilancia y de investigación privada, ya que se trata de servicios que potencialmente pueden incidir de forma directa en la esfera de la intimidad de los ciudadanos.

No están sujetas a esta Ley, las denominadas actuaciones de autoprotección (artículo 7.1), entendidas como el conjunto de cautelas o diligencias que se puedan adoptar o que ejecuten por sí y para sí mismos de forma directa los interesados (incluidas empresas), estrictamente dirigidas a la protección de su entorno personal o patrimonial, y cuya práctica o aplicación no conlleve contraprestación alguna ni suponga algún tipo de servicio de seguridad privada prestado a terceros.

El artículo 2 de la LSP recoge que **medida de seguridad** son aquellas disposiciones adoptadas para el cumplimiento de los fines de prevención o protección pretendidos, significando que los sistemas de videovigilancia o videograbación son medidas de seguridad electrónica, orientadas a detectar o advertir cualquier tipo de amenaza, peligro o presencia o intento de asalto o intrusión que pudiera producirse, mediante la activación de cualquier tipo de dispositivo electrónico.

La Orden INT/318/11 establece la formación sobre videovigilancia desde dos ámbitos: el primero, se refiere a la **formación previa** que se da a los Vigilantes de Seguridad y a los Directores de Seguridad en los módulos formativos, y el segundo, **formación permanente**, contenida en los planes de formación para el personal que desarrolla sus servicios en instalaciones como son las centrales nucleares o centros de internamiento y dependencias de seguridad, así como en eventos públicos y deportivos, entre otros.

La utilización de sistemas de videovigilancia en el ámbito de la seguridad privada repercute en actividades prestadas por empresas de seguridad, actuaciones de los despachos de detectives, medidas de seguridad de establecimientos obligados, bien por normativa bien por medida impuesta por la Autoridad competente.

El artículo 42 de la LSP dice que los **servicios de videovigilancia** consisten en el **ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.**

La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estarán sometidos a lo previsto en la normativa de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

Asimismo, las grabaciones realizadas por estos sistemas de videovigilancia, cuando se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, deben ser aportadas, bien de propia iniciativa o a requerimiento a las Fuerzas y Cuerpos de Seguridad (FF.CC.S.) competentes.

Son diversas las ocasiones en las que, en relación con lo anterior, las FF.CC.S. trasladan a las empresas de seguridad solicitudes de aportación de las imágenes procedentes de determinados clientes para incorporarlas en la tramitación de procedimientos judiciales o administrativos.

La LOPD en su artículo 22 dispone la recogida y tratamiento para fines policiales de datos de carácter personal por las FF.CC.S. sin consentimiento de las personas afectadas, limitado a aquellos supuestos de prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

Dado el elevado número de peticiones que surgen a nivel nacional sobre las imágenes que se han referido anteriormente, en el marco de los procedimientos descritos, la Policía Nacional ha establecido un **Protocolo de Colaboración con empresas de seguridad**, que permite una gestión más eficaz y eficiente de la solicitud y entrega de esas imágenes, a través de un portal web de gestión de grabaciones, que contiene esa información que habitualmente se entrega en mano para su tratamiento oportuno, permitiendo agilizar el proceso de solicitud, obtención y entrega de las imágenes interesadas por los investigadores, cumpliendo con todas las garantías de seguridad exigibles, así como salvaguardando la necesaria cadena de custodia.

A este Protocolo pueden adherirse, previo acuerdo entre las partes, otras Fuerzas y Cuerpos de Seguridad, así como empresas, entidades, corporaciones o grupos empresariales, en beneficio del servicio público que se debe prestar.

UNIDAD CENTRAL DE SEGURIDAD PRIVADA
R@S - Telf.: **913223951 -** Email: **redazul@policia.es**

3. La protección de datos de carácter personal.

El **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016** (**RGPD**), relativo a la protección de las personas 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 se aplica desde el **25 de mayo** del presente año 2018.

Este Reglamento, que es de aplicación directa, habilita a cada Estado miembro de la UE a adaptar al ordenamiento jurídico propio alguno de sus aspectos, lo que en el caso de España supone la futura aprobación de una nueva Ley Orgánica que sustituirá a la **Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).**

Según el artículo 3 de la **LOPD**, se entiende por:
a) **Datos de carácter personal**: cualquier información concerniente a personas físicas identificadas o identificables.
b) **Fichero**: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) **Tratamiento de datos**: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) **Responsable del fichero o tratamiento**: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
e) **Afectado o interesado**: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
f) **Procedimiento de disociación**: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
g) **Encargado del tratamiento**: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
h) **Consentimiento del interesado**: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
i) **Cesión o comunicación de datos**: toda revelación de datos realizada a una persona distinta del interesado.
j) **Fuentes accesibles al público**: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

El **RGPD** recoge, en su artículo 2, que se excluyen del ámbito de aplicación del mismo, entre otros, el tratamiento de los datos relacionados con la seguridad nacional, con la política exterior y de seguridad común de la UE, y el que se lleve a cabo por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención, según se refiere también dentro del ámbito de aplicación de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de fecha 27 de abril.

Las principales **novedades** que incorpora el **RGPD** son:

- **Principio de responsabilidad proactiva** (arts. 5.2 y 24).
- Modificación de las **condiciones para el consentimiento** del tratamiento de los datos (art.7).
- **Principio de transparencia** del responsable del fichero o tratamiento de los datos hacia el interesado en relación al conjunto de tratamientos realizados y los datos recogidos (art.12).
- **Ejercicio de los derechos** reconocidos a los interesados: **acceso, rectificación, supresión o derecho al olvido, limitación del tratamiento, portabilidad y oposición** (arts. 14 al 21).
- Obligación de tener un **Delegado de Protección de Datos** (art.37).
- Obligación de tener un **Registro de las actividades de tratamiento** (art.30). Sustituye la obligación de elaborar una Orden Ministerial y su posterior notificación a la Agencia Española de Protección de Datos.
- Obligación de **notificar la violación de seguridad** de los datos personales a la Autoridad de control y al interesado (arts. 33 y 34).
- Obligación de realizar un **análisis de impacto relativo a la protección de datos** (art.35).

Las conductas que afectan a la privacidad de las personas y a su derecho a la protección de datos, tienen dos ámbitos de actuación: el primero, desde el punto de vista penal, cuando fueran consideradas por la Autoridad Judicial como delito tipificado en el Código Penal; y el segundo, aquellos casos que no tienen consideración de delito pero en los que se aprecia que se ha vulnerado la normativa de protección de datos, constituyendo infracciones que den lugar a la instrucción de procedimientos administrativos.

Entre los hechos que constituirían una infracción a la normativa de protección de datos y que podrían ser objeto de sanción se encuentran:

- Conseguir los datos personales de una persona de manera ilícita, de forma engañosa o fraudulenta.
- Utilizar los datos de carácter personal de una persona o comunicarlos a un tercero sin su consentimiento, especialmente si se trata de ideología, religión, creencias, orientación sexual, salud, vida y origen étnico.
- Utilizar los datos de carácter personal de una persona para fines incompatibles con los que motivaron su recogida y sin su consentimiento.

Todo tratamiento de datos personales debe ser lícito y leal, y debe quedar claro para las personas físicas que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.

UNIDAD CENTRAL DE SEGURIDAD PRIVADA
R@S - Telf.: **913223951 -** Email: **redazul@policia.es**

4. Planes de Apoyo Operativo (PAO) en Infraestructuras Críticas.

La **Ley 8/2011, de 28 de abril**, establece las medidas para la protección de las infraestructuras críticas, teniendo como objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de las infraestructuras críticas. También recoge las especiales obligaciones que deben asumir tanto las Administraciones Públicas como los operadores de las infraestructuras que se determinen como críticas.

Las **infraestructuras estratégicas** son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales que son aquellos servicios necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

Las **infraestructuras críticas** son aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

La **protección de infraestructuras críticas** es el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas recoge, entre otros, los **Planes de Apoyo Operativo**, que son los **documentos operativos donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los Operadores Críticos para mejorar la eficacia en la protección de las infraestructuras críticas.**

Por cada una de las infraestructuras críticas e infraestructuras críticas europeas dotadas de un **Plan de Protección Específico** y sobre la base a los datos contenidos en éste, la Delegación del Gobierno en la Comunidad Autónoma o, en su caso, el órgano competente de la Comunidad Autónoma, supervisará la realización de un Plan de Apoyo Operativo por parte del Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate.

En relación con los correspondientes Planes de Protección Específicos (PPE), los Planes de Apoyo Operativo deberán contemplar, si las instalaciones lo precisan, medidas planificadas de vigilancia, prevención, protección y reacción que deberán adoptar las unidades policiales y, en su caso, de las Fuerzas Armadas, cuando se produzca la activación del Plan Nacional de Protección de las Infraestructuras Críticas, en función del nivel de alerta que se encuentre establecido, o bien de confirmarse la existencia de una amenaza inminente sobre dichas infraestructuras. Estas medidas serán siempre complementarias a aquellas de carácter gradual que hayan sido previstas por los operadores críticos en sus respectivos Planes de Protección Específicos.

El CNPIC verificará los contenidos mínimos de los Planes de Apoyo Operativo, así como el modelo en el que fundamentar la estructura y desarrollo de éstos, que se basará, en la parte que les corresponda, en la información contenida en los respectivos Planes de Protección Específicos.

Los PAO cuentan con dos partes: la primera elaborada con los datos aportados por el **Operador Crítico** que constan en el Plan de Protección Específico redactado por él, donde la figura del Delegado de Seguridad es específica y obligatoria en cada infraestructura crítica, con independencia de que resulte ser el Director de Seguridad, del Departamento de Seguridad, o que ejerza también la figura de enlace; y la segunda, elaborada por las **Fuerzas y Cuerpos de Seguridad** competentes con datos exclusivamente policiales.

Los datos del Operador Crítico establecen las medidas organizativas de la instalación (organigrama, estructura, personal y medios de seguridad privada), las medidas y medios de seguridad disponibles, y la planificación de las medidas de seguridad.

Los datos de las Fuerzas y Cuerpos de Seguridad competentes recogerán los dispositivos específicos planificados (designación de responsables, canales y medios de comunicación y los protocolos de actuación conjunta, incluyendo las actuaciones con otras Fuerzas policiales), y se graduarán y clasificarán en función de la situación de normalidad, el nivel de activación nacional o local de los Planes de Prevención y Protección Antiterrorista y del sistema de Protección de las Infraestructuras Críticas, y la amenaza sobre una infraestructura concreta. La planificación y previsión de los dispositivos, la designación de los medios y recursos, así como el despliegue estratégico del PAO corresponde al responsable de la Brigada Provincial o Local de Seguridad Ciudadana de la Policía Nacional, o al responsable de la unidad homóloga en la Guardia Civil.

UNIDAD CENTRAL DE SEGURIDAD PRIVADA
R@S - Telf.: **913223951 -** Email: **redazul@policia.es**

5. El síndrome del estrés postvacacional.

El **estrés** es una respuesta normal del organismo a las demandas del ambiente. Cuando esas demandas superan nuestras estrategias de afrontamiento, es cuando aparece el estrés.

Durante las vacaciones nos olvidamos de los horarios establecidos durante la rutina laboral, desconectamos a nivel mental y emocional, reducimos el uso de la tecnología, teléfono, ordenador, correos, etc., y esta desconexión es fundamental para proteger nuestro bienestar físico y psicológico, tanto en el ámbito personal como en el laboral.

El **síndrome del estrés postvacacional** es lo que se conoce popularmente como el estrés que experimenta el individuo al incorporarse al trabajo tras las vacaciones. No está considerado un trastorno como tal en los manuales diagnósticos pero sí que puede conllevar algún tipo de consecuencia a largo plazo si no lo reconocemos, lo normalicemos y actuemos sobre él.

¿Por qué nos cuesta tanto volver al trabajo después de disfrutar de unas merecidas vacaciones?

Cuando regresamos al trabajo tenemos que volver a adaptarnos a una nueva situación, a las nuevas demandas que nos ofrece el ambiente, a cambiar nuestro estilo de vida, y ahí es cuando el organismo puede empezar a experimentar cambios tanto a nivel fisiológico (aumento de la tasa cardiaca, sudoración, tensión muscular, respiración agitada y superficial…), cognitivo (valoraciones irracionales, pensamientos negativos, incapacidad de tomar decisiones, falta de concentración, olvidos frecuentes,…), motor (bloqueo/paralización, aumento del tiempo de reacción, precipitación en las acciones,…) y emocional (ansiedad, irritabilidad/ira, embotamiento, tristeza,…).

Es importante saber reconocer las respuestas de nuestro organismo al estrés para poner en marcha recursos de afrontamiento y adaptarnos a la nueva situación cuanto antes, ya que pueden verse afectados diferentes ámbitos de nuestra vida, no sólo en el ámbito laboral sino también en el familiar y en el personal.

Hay personas que pueden vivir esta situación con más intensidad que otras, ya que se les puede acumular varios estresores como, por ejemplo, dificultades económicas, problemas de pareja, enfermedades, acoso psicológico por parte de los compañeros, etc.

"La verdadera clave del estrés no es tanto qué nos ocurre sino cómo vivimos lo que nos ocurre"

Aunque no se requiere tratamiento, si no ponemos remedio puede llegar a provocar algún tipo de trastorno de ansiedad o del estado de ánimo (como depresión) e incluso una baja laboral, ya que nuestro organismo no aguantaría un largo periodo de tiempo este nivel tan alto de activación y nos llevaría al agotamiento, tanto físico como mental. Aunque no todo el mundo responde de la misma manera a este estresor, hay personas que ven con ilusión la vuelta al trabajo.

"Un aval para la salud es aprender a cuidar nuestro cuerpo tanto física, como psíquica como socialmente"

Volver a enfrentarse a responsabilidades, horarios fijos y obligaciones, puede causarnos ansiedad si no disponemos de estrategias de afrontamiento adecuadas.

- Establecer un **horario más o menos fijo** de descanso, de comidas y de ejercicio físico, dedicarnos tiempo a nosotros mismos, es la mejor opción para volver a la rutina cuanto antes, al fin y al cabo se trata de un proceso de adaptación al medio.
- Hay que **darle tiempo a nuestro cuerpo y a nuestra mente** a readaptarse, puede que los primeros días estemos menos motivados o nos sintamos con las energías más bajas de lo habitual, todo esto es normal.
- **Empezar** poco a poco con la tarea, **progresivamente**, con lo que más nos motiva, priorizar y organizarse el tiempo son pautas que nos ayudarán a llevar una mejor adaptación a la rutina laboral. Pero también hay cosas agradables en la vuelta al trabajo como, por ejemplo, el volver a ver a los compañeros después de un tiempo, si estas relaciones son positivas, las reacciones de estrés van a ser menos intensas.
- **Potenciar las relaciones sociales**, practicar nuestras **habilidades sociales**, aprender a distinguir lo urgente de lo que no lo es, saber decir que no y poner límites, son pequeñas acciones que nos ayudarán a enfrentarnos a situaciones que potencialmente pueden causarnos estrés.

"No es el más fuerte ni el más inteligente el que sobrevive, sino el que responde mejor al cambio"
(Charles Darwin)

UNIDAD CENTRAL DE SEGURIDAD PRIVADA
R@S - Telf.: **913223951 -** Email: **redazul@policia.es**

6. INFORME TÉCNICO: Diseño de un Curso de Introducción a las TIC corporativas[1]

La formación dentro de cualquier entorno laboral es un pilar fundamental en el proceso de capacitación de los trabajadores. En la familia de normas ISO9000 [2], se subraya la importancia de la gestión de los recursos humanos, recogiendo la necesidad de una formación apropiada. La norma UNE66915 [3] desarrolla el proceso formativo de las organizaciones, buscando que el trabajador esté cualificado en todo momento para cumplir con la misión asignada dentro de la organización y que así sea capaz de proporcionar productos o servicios de calidad en un entorno de competencia que además está en continua evolución. Este informe es una adaptación del TFM del autor proponiendo la necesidad de un curso que habilite a los trabajadores de cualquier empresa para su primer contacto con las TIC corporativas, o para suplir el desconocimiento de aspectos básicos de éstas en trabajadores veteranos en la empresa.

1.Introducción.

Las colecciones de normas de calidad nos proponen una herramienta para armonizar todos los procesos de una organización. Estas herramientas entre sus múltiples ventajas ofrecen unos procesos que comparten miles de empresas y que han sido pulidos de forma consensuada.

Este informe se basa en las directrices marcadas por la ISO 9001, en su punto 6.2 “Recursos humanos”, y especialmente el punto 6.2.2 “Competencia, toma de conciencia y formación”, en el punto 8.2.2 “Auditoría interna” de la misma norma, y en la Norma UNE 66915 “Directrices para la Formación”.

En un entorno ideal, el cumplimiento de la norma precisa la implicación directa de los distintos departamentos, sin embargo, en un entorno real es necesario que el departamento que planifica un curso supla los puntos que no pueden cumplirse por parte de distintos actores que, por diversos motivos, no pueden realizarlos. Esta carencia en la planificación de un curso TIC se puede suplir con la experiencia y conocimientos acumulados por el departamento que planifica el curso, además de un análisis profundo de las incidencias que se atienden desde el Departamento de Informática.

Es de señalar, que la bibliografía científica para el proyecto que tratamos se centra en las guías de aplicación de las normas, más que en estudios detallados, siendo escasas las referencias para la Administración Pública, habiéndose basado el autor principalmente en el “Libro blanco para la mejora de los servicios públicos” [4], el libro “Seguimiento de la competencia y del proceso de formación” [5], y la “Guía de calidad y mejora en las administraciones públicas” [6].

1.1. Justificación de la necesidad del proyecto

Por conocimiento profesional se han detectado numerosas carencias en distintos proyectos y empresas, siendo, siendo los propios trabajadores de los departamentos informáticos los que solicitan la realización de un curso de formación que debería contemplar entre otros aspectos:

a) Formación del trabajador.
b) Que tenga una aproximación inicial al entorno TIC de la Organización.
c) Que adquiera una capacitación básica de las herramientas TIC.
d) Que conozca procedimientos y formularios comunes.
e) Que conozca las medidas de seguridad básicas.
f) Que sepa utilizar el carnet profesional y sus certificados electrónicos, u otras credenciales de acceso, así como el reseteo de claves u otras incidencias relativas a este aspecto.
g) Reducción del número de incidencias.
h) Que los usuarios conozcan el ciclo de vida de las incidencias informáticas.
i) Reducción de llamadas al departamento TIC, favoreciendo las incidencias por escrito para poder realizar un seguimiento efectivo, una estadística más fiable que permita ser reactivos a las problemáticas que se puedan detectar en su análisis, y la revisión constante de procedimientos e instalaciones, pudiendo planificar los mantenimientos preventivos.

1.2 Descripción.

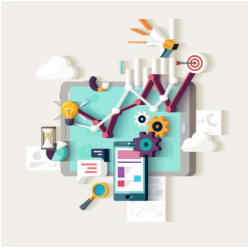
Aunque el proyecto tiene su origen en la demanda del personal de un entorno concreto, es aplicable a cualquier entorno corporativo. Esta demanda de formación transmitida tanto al departamento TIC como al departamento de Formación, se materializa en una petición por parte del Departamento de Formación de estudiar la viabilidad, recursos necesarios, temario, contenido, método de evaluación, calendario… en definitiva, se pide al departamento TIC el Diseño de un Curso de introducción a las TIC corporativas.

1.3. Entorno

Este informe está basado en un caso real situado en una empresa de Madrid dirigido a 500 personas encuadradas en la gestión de la dependencia, y desarrollado a través de varias ediciones.

1.4. Contexto

Organismo Central o dependencias centrales de una empresa, pudiendo extenderse a organismos no centralizados dependiente de ella que realiza labores similares. El patrón es extrapolable a cualquier empresa.



2. Estado de la cuestión

La colección de normas ISO 9000 permiten la implantación de sistemas de Calidad para todo tipo de organizaciones, permitiendo que los procesos de éstas sean verificables con unos mismos criterios e incluso que se puedan implementar procesos comunes. En nuestro caso en concreto, de detecta una carencia en el ámbito de las TIC, extrapolable a la mayoría de las empresas. Esta carencia se asume como una limitación normal en el entorno laboral en la mayoría de las empresas.

La aplicación de la norma establece claramente que se deben establecer las competencias y evaluar sus carencias, y éste es el punto clave que suele fallar en todas las empresas. La mayoría de ellas aplican este punto a la hora de la contratación, pero no hacen un seguimiento durante la vida laboral de los cambios en las competencias ni se evalúan las carencias. Ésta es una **función claramente directiva**, que en un entorno real se debe complementar con la experiencia del departamento TIC, ya que es el que recibe las dudas en la utilización de los medios y aplicaciones que utiliza el trabajador.

Las normas son una herramienta muy útil, pero muy difíciles de aplicar cuando no se implican todos los departamentos de una empresa. En muchos casos, la realidad impone que primero hay que poner en marcha los ciclos, y una vez demostrada la eficacia y bondad de los estándares, incorporar a los distintos actores implicándoles en las tareas necesarias que establece las normas. Es decir, en mi opinión en un principio es preferible iniciar la implantación de cualquier estándar (en este caso el referente a la formación, y perfeccionarlo con el paso de las ediciones del curso que se realicen, dejando que la eficacia del trabajo realizado sume a los distintos actores), que dejar que la complejidad de las normas ahogue su implantación o la retrase indefinidamente.

Cuando una persona o departamento detecta una carencia, deben buscarse los medios necesarios para resolverlos, y no se puede escudar en las jerarquías, las organizaciones, las competencias o los problemas, para posponer las soluciones. La implicación y el deseo de mejora de las empresas y procedimientos implican que el compromiso se materialice en la búsqueda de los medios para que los proyectos sean exitosos, aunque para ello se deba ir más allá del propio deber y no se sea exhaustivo en la aplicación de la norma.

El problema detectado es un problema muy extendido en gran cantidad de empresas, normalmente más extendido en las empresas de tamaño medio. En los procesos selectivos se da mucha importancia a las capacidades técnicas y conocimientos informáticos de los aspirantes, sin embargo, no suele contemplarse una formación inicial y reglada sobre el entorno y los medios TIC corporativos, por lo que el nuevo trabajador los aprende de forma autodidacta o con la ayuda de compañeros más veteranos, que muchas veces tampoco tienen un conocimiento exacto y completo de aquello que está transmitiendo.

2.1. Antecedentes

Para la realización de este proyecto tenemos como base los documentos propios de cualquier organización, los formularios que se utilizan para distintas tareas que se deben de introducir en el curso, procedimientos internos, y documentos de difusión en el ámbito que nos ocupa.

Es necesario que cualquier curso TIC incluya como parte importante un módulo de seguridad, y que éste aborde la utilización de los medios TIC tanto en el entorno laboral, como en el personal.

Es preferible realizar una jornada básica que aborde las nociones básicas de las TIC en el entorno corporativo, a que por realizar un curso con más carga lectiva no se pueda llevar a la práctica por falta de recursos. Por ello, inicialmente el autor apuesta por unas jornadas que sean muy divulgativas, con conceptos claros y sencillos para lograr una verdadera eficacia.

3. Desarrollo del trabajo

3.1. Alcance

El proceso de Diseño, desarrollo e implantación del curso. Tiene su entrada en la petición del Departamento de Formación, que por requerimiento de la División de formación debe facilitar una serie de documentación estandarizada para que se estudie la viabilidad del curso. Una vez aprobada la viabilidad se debe realizar toda la documentación relativa al curso o jornadas informativas. Además se propondrán dos horarios, uno utilizando las primeras horas de la jornada laboral, para que el trabajo de los departamentos se vea aceptado el mínimo posible, y un segundo horario intensivo.

3.2. Metodología/Tecnología/Modelos

Se basará en las directrices marcadas ISO 9001, en su punto 6.2 Recursos humanos, y especialmente el punto 6.2.2 Competencia, toma de conciencia y formación.

La Norma UNE 66915 desarrolla las “Directrices para la Formación” de la familia de normas ISO 9000. El proceso queda establecido según el esquema representado en la Fig.1.

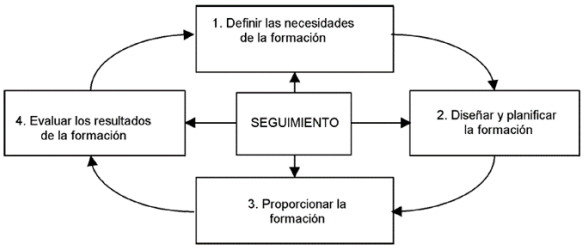


Fig. 1. Fases de la formación

Este proceso se puede explicar sencillamente de la siguiente manera, puesto que los pasos a seguir los define perfectamente la norma y considero que la simple reproducción de los puntos de la Norma sería banal.

La implicación en la primera fase de la dirección es fundamental, el proceso empieza por una definición exacta de las necesidades de conocimientos y habilidades para cada puesto de trabajo, se denominan “competencias”.

Una vez definidas claramente las competencias se debe evaluar si los trabajadores cumplen los requisitos establecidos, las competencias, y se deben establecer los incumplimientos, que la Norma denomina “**carencias**”.

Hay que plantear las soluciones para las carencias detectadas, en este caso aquellas que se pueden subsanar mediante la formación, y una vez definidos claramente todos estos puntos podemos pasar a la siguiente fase, que es el diseño y planificación de la formación.

Para la definición de la formación:

1º. Analizar las limitaciones que tenemos, siendo necesaria la implicación de la dirección, y que precisamente es un punto a impulsar según el punto 5 de la ISO 9001:2008 Responsabilidad de la dirección”, y especialmente el punto 5.6, “Revisión por la dirección”, para ayudar a la Dirección en

se propone una auditoría interna que debe ser evaluada por ésta.

2º. Elegir el método de formación y los formadores. En este caso la formación será presencial, con formadores que pertenecen a la plantilla de la empresa, concretamente al Departamento de Informática, con carácter voluntario.

3º. Definir los objetivos, de forma que la formación responda a las necesidades detectadas y se puedan subsanar las carencias, recogiéndolas en un documento.

4º. Definir el calendario, hemos establecido tres ediciones del curso anuales, dentro del ciclo de un año escolar (septiembre-julio) incluyendo las tareas propias de cada edición del Curso y añadiendo procesos que engloban todo el curso, principalmente la evaluación de los objetivos y la auditoría interna. Para la planificación se debe tener en cuenta las épocas con más carga laboral, así como los periodos vacacionales, para no sustraer del servicio personal que sea necesario o imprescindible en determinadas épocas.

5º. Evaluar los requisitos de personal y financieros. Para una jornada o un curso reducido, se establece que con un profesor titular y uno suplente es suficiente, aunque por motivos prácticos se repartirá el programa entre al menos dos profesores que deberán dominar todo el temario de manera que se puedan intercambiar. Los profesores se irán intercalando durante el Curso para contribuir al dinamismo de éste. El coste de la formación se puede calcular según el modelo de Kirkpatrick, siguiendo para ello el modelo de aplicación expuesto en artículo "Evaluación e implantación de un modelo de evaluación de acciones formativas" [7], teniendo en cuenta que se realiza enteramente con recursos propios, computando los gastos teniendo en cuenta el coste del sueldo/hora tanto del profesorado como de los alumnos, así como el coste que se pueda imputar a la utilización del aula, los medios audiovisuales, desplazamientos, mantenimiento de las instalaciones...

6º. Establecer los criterios de evaluación que nos permitirán medir la eficacia de la acción formativa, y esto se materializa en un cuadro de mandos balanceado.

7º. Los últimos puntos de la norma hablan de la evaluación, apoyo, y seguimiento del plan formativo, que en nuestro caso corresponderán principalmente al Departamento de formación y que debe incluir un plan de auditoría interna.

4. Conclusiones

Al realizar este proyecto hay que tener en cuenta dos vertientes que se comunican y se complementan mutuamente: la primera es la necesidad de formación de los funcionarios, y la segunda, el trabajo del Departamento de Informática.

El departamento TIC suele adolecer de una falta de personal constante en la mayoría de las empresas que impide poder realizar su labor con la excelencia deseada tanto por su jefatura como por su personal, como tantos otros departamentos, agravado por la falta de personal técnico cualificado y el intrusismo.

Mediante este proyecto se confía en conseguir una mayor formación del usuario, una mejora de la imagen de los departamentos implicados, una reducción del número de incidencias, y una mejora de sinergias entre TIC y usuarios.

La visión negativa que tienen muchos usuarios de la Informática, mediante la formación, se espera revertir, y que los usuarios puedan valorar las herramientas que se ponen a su alcance como facilitadoras de su trabajo.

La consecución en la reducción del número de incidencias, y la disminución de incidencias vía telefónica, permitirá al departamento TIC una mejor planificación de su tiempo, una mayor eficiencia de medios, y una mejora en los tiempos disponibles para la formación.

Sin embargo el protagonista principal de este curso es la Organización, que es la que se beneficia mediante la capacitación de sus trabajadores. Son los trabajadores que van a mejorar su nivel de competencia los principales beneficiarios, que además van a poder desarrollar su trabajo de una forma más eficaz, con menos "miedo" a la informática, comprendiendo mejor las máquinas que deben facilitar su trabajo y que, sin embargo, sienten que a veces parecen dificultarlo. Van a conocer los medios que tienen a su alcance, van a saber cuándo y cómo solicitar la intervención del Departamento de Informática, que es una parte importante en cualquier Organización moderna y cuya principal seña de identidad debe ser el servicio.

Por último señalar que aunque puede parecer que el planteamiento del Curso es demasiado sencillo, a veces, nos encontramos que las soluciones más evidentes y sencillas, las que tenemos al alcance de la mano, son las más efectivas

5. Referencias

1. Este informe es una adaptación del artículo del mismo autor presentado en el Congreso "ATICA2017 Tecnología. Accesibilidad. Educar en la sociedad red", págs. 366-373, Sevicio de publicaciones de la Universidad de Alcalá, ISBN: 978-84-16599-50-9

2. *ISO9001:2015 - Quality Management Systems*

3. *UNE 66915:2001 - Gestión de la calidad. Directrices para la formación*.

4. *Libro blanco para la mejora de los servicios públicos*. MAP. (2002)

5. *Seguimiento de la competencia y del proceso de formación.* Pierre Massot y Daniel Feisthammel. Editorial: AENOR. (2003)

6. *Guía de calidad y mejora en las administraciones públicas*. Tomás Rodríguez Garraza. Instituto Navarro de Administración Pública. (2005)

7. *Evaluación e implantación de un modelo de evaluación de acciones formativas*. Mª. Lourdes Jiménez. Roberto Barchino. Universidad de Alcalá, Departamento de Ciencias de la Computación, 28871 Alcalá de Henares, España {lou.jimenez, roberto.barchino}@uah.es https://www.researchgate.netpublication/228854838_Evaluacion_e_implantacion_de_un_modelo_de_evaluacion_de_acciones_formativas [accessed Jul 25, 2017]

(Policía Luis M. A., Área Informática Policía Nacional)

7. FORMACIÓN:

JORNADAS FORMATIVAS DE PREVENCIÓN ANTITERRORISTA E INTERLOCUTOR POLICIAL SANITARIO EN DIFERENTES LOCALIDADES ESPAÑOLAS

La Policía Nacional, a través de la Unidad Central de Seguridad Privada, en colaboración con la Comisaría General de Información y con Unidades de diversas Jefaturas Superiores, tiene programadas unas jornadas sobre formación, prevención y protección antiterrorista, así como de prevención de agresiones al personal sanitario dirigidas al personal que integra la Seguridad Privada en España.

Estas jornadas tienen como finalidad llevar a cabo la función que tiene encomendada la Policía Nacional, a través de la Unidad Central de Seguridad Privada y de las Unidades Territoriales de Seguridad Privada, de la formación permanente especial al sector de la Seguridad Privada, al objeto de impartir las instrucciones o pautas de actuación para hacer efectivo el principio básico de auxilio, colaboración y coordinación.

Las jornadas están distribuidas en varios formatos, al objeto de dar cobertura a las diferentes necesidades que se plantean a los integrantes del sector de la Seguridad Privada:

- **Directores de Seguridad y Jefes de Seguridad**, la Comisaría General de Información impartirá el análisis de la amenaza terrorista, la situación del yihadismo internacional, ciberterrorismo y ciberseguridad, y la actualización del Plan Integral de Colaboración entre la Policía Nacional y Seguridad Privada.

- **Vigilantes de Seguridad y Escoltas**, personal de la Unidad Central de Seguridad Privada, junto con TEDAX-NRBQ de la Brigada Provincial de Información y Unidades de Intervención Policial (UIP) o Unidades de Prevención y Reacción (UPR) de la Brigada Provincial de Seguridad Ciudadana, transmitirán las recomendaciones sobre la prevención y actuación en caso de atentado terrorista, búsqueda, localización y detección de artefactos explosivos y actuaciones operativas como la detención e identificación en el ejercicio de su profesión.

- **Detectives**, personal de la Unidad Central de Seguridad Privada planteará cuestiones normativas y operativas para su trabajo diario conforme a la legislación vigente.

- **Centros de Formación** de Seguridad Privada, personal de la Unidad Central de Seguridad Privada les informará sobre temas relacionados con la formación de los vigilantes (formación previa y de actualización) y con el cumplimiento de los requisitos de apertura y funcionamiento de los centros.

- **Personal sanitario** (médicos, enfermeros, auxiliares, celadores, etc.) se les informará por el Interlocutor Policial Nacional Sanitario y su equipo de una serie de recomendaciones de actuación para prevenir y, en su caso, controlar, los incidentes que en el ámbito sanitario pudieran producirse con pacientes y sus familiares.

A continuación se relacionan los lugares y fechas de celebración de las próximas jornadas, para que puedan solicitar información y tramiten su inscripción, en caso de ser de su interés, en las Unidades Territoriales de Seguridad Privada que se relacionan.

ALGECIRAS

Días 18 y 19 de septiembre de 2018
Formato: Directores y Jefes de Seguridad, Vigilantes de Seguridad, Personal sanitario.
Unidad Territorial Seguridad Privada
Dirección: Avda. del Embarcadero, s/n
Teléfono: 956588437
Email: algeciras.segpriv@policia.es

CEUTA

Días 20 y 21 de septiembre de 2018
Formato: Directores y Jefes de Seguridad, Vigilantes de Seguridad, Personal Sanitario.
Unidad Territorial Seguridad Privada
Dirección: Avda. San Juan de Dios, nº 11
Teléfono: 956513418
Email: ceuta.segpriv@policia.es

OVIEDO

Días 26 y 27 de septiembre de 2018
Formato: Directores y Jefes de Seguridad, Vigilantes de Seguridad, Detectives, Centros de Formación y Personal Sanitario.
Unidad Territorial Seguridad Privada
Dirección: Avd. Buenavista, s/n
Teléfono: 985967171
Email: oviedo.segpriv@policia.es

*"ALLÁ DONDE ESTÉ LA **SEGURIDAD PRIVADA**, ESTÁ LA **POLICÍA NACIONAL**"*

UNIDAD CENTRAL DE SEGURIDAD PRIVADA
R@S - Telf.: **913223951 -** Email: **redazul@policia.es**