

# BOLETÍN R@S

UNIDAD CENTRAL DE SEGURIDAD PRIVADA



## PORTADA

Página 1

## SEGURIDAD PRIVADA REPRESENTADA EN EL DÍA DE LA POLICÍA

Página 2 - 3

## PERSONAL DE SEGURIDAD PRIVADA CONDECORADO EN EL DÍA DE LA POLICÍA

Página 4

## LA VENTANA DEL R@S

Página 5 - 6

## ¿COMO ESTABLECER UNA CULTURA DE SEGURIDAD EN LA EMPRESA?

Página 7 - 8

## PROTOCOLO DE DENUNCIAS IN SITU: PROPUESTA DE AMPLIACIÓN A LAS AGRESIONES A LOS PROFESIONALES SANITARIOS

Página 9

## LOS PASADORES DE LAS MENCIONES HONORÍFICAS DEL PERSONAL DE SEGURIDAD PRIVADA

Página 10

## PREGUNTAS FRECUENTES

Página 11 - 13

## NOTICIAS

Página 14 - 19

# EL DÍA DE LA POLICÍA MÁS CERCA DE LA SEGURIDAD PRIVADA



# SEGURIDAD PRIVADA REPRESENTADA EN EL DÍA DE LA POLICÍA

El día 2 de octubre se celebra el Día de la Policía, fiesta de la Policía Nacional. Este año, los actos centrales se desarrollaron en la ciudad de Valladolid.

Desde el 17 al 24 de septiembre estuvo en la Acera de Recoletos de la capital vallisoletana la exposición "Medios y museo de la Policía" en la que los ciudadanos pudieron conocer los diferentes vehículos policiales históricos y actuales allí dispuestos. La misma se completaba con varios puestos de diferentes unidades de la Policía Nacional, estando presentes **por primera vez las Unidades de Seguridad Privada** representadas por la Unidad Central de Seguridad Privada de la Comisaría General de Seguridad Ciudadana.

Para la exposición, la Unidad Central elaboró un video que daba a conocer a la ciudadanía lo que es la seguridad privada, haciendo un recorrido por su historia, desde sus inicios hasta la actualidad, con especial hincapié en los momentos que el sector ha vivido junto a Policía Nacional. El video se proyectaba en el "stand" de la Unidad Central a lo largo de toda la jornada, habiéndose recibido más de 2500 visitas entre las que se encontraban profesionales de la seguridad privada. Con ello se acercó este sector a la ciudadanía, explicando su importancia en el buen desarrollo de las diferentes actividades sociales y la estrecha relación que mantiene con la Policía Nacional.

También se explicó a los visitantes la figura del Interlocutor Policial Sanitario y a los profesionales de la salud que se acercaron se les informó sobre los consejos para prevenir agresiones en su lugar de trabajo, entregándoles un documento desplegable elaborado por la Policía Nacional en el que se recogen los mismos.





# SEGURIDAD PRIVADA REPRESENTADA EN EL DÍA DE LA POLICÍA



# PERSONAL DE SEGURIDAD PRIVADA CONDECORADO EN EL DÍA DE LA POLICÍA

El 6 de octubre la Comisaría General de Seguridad Ciudadana llevó a cabo, en el complejo policial de Moratalaz, su acto de celebración del Día de la Policía.

En el mismo se impusieron las Medallas al Mérito Policial a los integrantes de esta Comisaría General reconocidos por su labor durante el presente año. Asimismo, se han entregado, a propuesta de la Unidad Central de Seguridad Privada, cuatro medallas a personal de seguridad privada.

**!!! ENHORABUENA A LOS CONDECORADOS !!!**



**Santiago García San Martín**



**Silvia San Martín Álvarez**



**Luís Carlos Bunes Molina**



**Mariano Agüero Martín**





## FENOMENOLOGÍA DELINCUENCIAL: FRAUDE AL CEO

**AUTOR: CRISTÓBAL ALZAMORA MORENO**

El “fraude del CEO”, incluido en el denominado Business Compromise Fraud (BEC, por sus siglas en inglés), es una tipología basada en técnicas de ingeniería social, que utiliza el factor humano como eslabón más débil de la seguridad, y que tiene como objetivo el engaño de empleados, con acceso a los recursos económicos de la empresa objetivo, para que realicen una transferencia de dinero desde la cuenta corporativa, saltándose los protocolos de control establecidos (EUROPOL EC3, s.f.).

La solicitud suele plantearse como una urgencia y/o con confidencialidad entre el CEO y el empleado, de manera que se dificulte cualquier tipo de comprobación. Los atacantes suelen seguir procedimientos corporativos, usar lenguaje típico de la empresa, etc. para ganarse la confianza de la víctima (UTPJ GC, 2016).

En términos generales, los esquemas de BEC, suelen presentar tres fases (IEWG, 2019):

**Fase 1. Obtención de información y acceso a las cuentas de correo electrónico de la víctima:** Los delincuentes recopilan toda clase de información y documentación relativa a la víctima y la empresa objetivo, pudiendo acceder ilegalmente a cuentas de correo electrónico o a dispositivos electrónicos, a menudo a través de ingeniería social o de técnicas de hacking.

**Fase 2. Transmitir instrucciones de transacciones de manera fraudulenta:** Los delincuentes utilizan la información robada a la víctima para enviar por correo electrónico instrucciones fraudulentas de pago o transmisión de datos a la institución financiera, tal como lo haría la víctima, utilizando la cuenta de correo electrónico de la víctima (en caso de controlarla) o crean una cuenta falsa que se le parece. El delincuente puede adjuntar documentos de respaldo, falsificados o robados a la víctima, a fin de mejorar su aparente legitimidad.

**Fase 3. Ejecutar transacciones no autorizadas:** Los delincuentes engañan al empleado o a la institución financiera de la víctima para que realicen transferencias que parecen legítimas pero que, de hecho, no

están autorizadas o son fraudulentas, en muchos casos obviando los controles establecidos por la propia empresa o entidad financiera.

Los pagos se suelen realizar a cuentas radicadas en instituciones financieras extranjeras (IEWG, 2019).

### Otras tipologías de BEC

#### **- Suplantación de identidad de un cliente comercial de una institución financiera**

El delincuente accede ilegalmente a la cuenta de correo electrónico de un empleado de la organización, o crea una parecida, y la utiliza para enviar instrucciones sobre transferencias fraudulentas a la institución financiera de esta.

#### **- Suplantación de identidad de un proveedor**

El delincuente suplanta la identidad de un proveedor de la organización y le envía a esta un mensaje de correo electrónico para informarle que los pagos de facturas o depósitos futuros deben realizarse a un nuevo número de cuenta, radicada en otro lugar.

#### **- Intervención en trámites inmobiliarios**

El delincuente compromete la cuenta de correo electrónico de una de las partes, o intermediario, de una operación inmobiliaria con el fin de alterar las instrucciones sobre el pago y desviar los fondos de la transacción o de las comisiones de los intermediarios.

### Ingeniería Social

Podemos definir la ingeniería social, en términos de seguridad, como: el empleo de técnicas y acciones premeditadas que permitan influir y/o manipular las acciones de las personas para obtener información o lograr que realicen tareas que, naturalmente, no harían.

# LA VENTANA DEL R@S

## FENOMENOLOGÍA DELINCUENCIAL: FRAUDE AL CEO

**AUTOR: CRISTÓBAL ALZAMORA MORENO**

Los ataques de ingeniería social dirigidos conllevan un proceso de obtención de información previo y un análisis en profundidad que podrá incluir, entre otros:

- Estructura, funcionamiento y organigrama de la organización.
- Relaciones comerciales y con otros terceros.
- Protocolos de seguridad de la organización y vulnerabilidades.
- Información y patrones de comportamiento de las víctimas.
- Obtención de modelos de documentación de la organización y de las víctimas.
- Patrones de comunicación corporativa.

Además de técnicas de ingeniería social, hacking e infecciones de malware, se pueden utilizar:

- Técnicas de acceso físico a instalaciones o dispositivos electrónicos.
- Técnicas de vigilancia personal o mediante medios tecnológicos.
- Técnicas OSINT para la obtención de información.
- Compra de información en el mercado negro para su explotación.
- Trashing físico (revisión de basura).
- Técnicas de clonado de dispositivos o tarjetas sim.



### La confianza como vulnerabilidad

Una de las vulnerabilidades explotada con mayor asiduidad por los delincuentes es la confianza que, entre otras, puede ser generada por las siguientes situaciones:

- **Origen conocido correos electrónicos, mensajes, documentos o dispositivos usb recibidos.** Que el remitente sea conocido y con contacto frecuente, o perteneciente a una Administración u organismo oficial, o que se utilicen plataformas de confianza y calificadas de seguras, facilita que el receptor no dude de su legitimidad o procedencia.
- **La pertenencia a determinados colectivos de las personas con las que se interactúa.** El hecho de portar un determinado uniforme puede facilitar que las personas no duden de la presencia de un individuo en determinados espacios o que sean más propensas a facilitar información.
- **La apariencia, simpatía, sexo y seguridad de la persona con la que se interactúa,** puede facilitar que la víctima vea a un individuo como más confiable.

### Formación y concienciación

Una de las premisas más importantes en ciberseguridad es que no existen "vigilantes eficaces" más allá de nosotros mismos. Regular nuestro comportamiento on-line, capacitarnos y poner los medios necesarios para dificultar al delincuente la consecución de sus objetivos son las mejores medidas de prevención, es decir, LA FORMACIÓN Y LA CONCIENCIACIÓN.

# ¿CÓMO ESTABLECER UNA CULTURA DE SEGURIDAD EN LA EMPRESA?

FUENTE: INCIBE

Bajo el lema “una cadena es tan fuerte como su eslabón más débil”, el INCIBE aborda en un nuevo dossier la cultura de seguridad en la empresa, concienciando de que es necesario invertir en la formación en ciberseguridad de los usuarios finales de los sistemas de información de cada entidad.

**EL USUARIO ES EL ESLABÓN MÁS IMPORTANTE DE LA CADENA DE LA SEGURIDAD**



El desarrollo, junto con la integración de una cultura de seguridad dentro de una organización, es un proceso complejo, dilatado en el tiempo que, además, requiere que los empleados interioricen unas pautas de actuación en sus actividades rutinarias que garanticen la seguridad de la información. De acuerdo con esto, la percepción que tienen estos trabajadores sobre los protocolos de ciberseguridad es generalmente negativa, creyendo que se trata de procedimientos que dificultan sus labores.

Para tratar de reducir al máximo estas incomodidades, la empresa debe de establecer las siguientes recomendaciones:

## 1. FORMACIÓN EN SEGURIDAD

Es habitual que la formación en seguridad de la información en las organizaciones sea nula, a pesar de que el Reglamento General de Protección de Datos considere obligatoria la formación de los empleados en materia de seguridad de los datos personales. Adicionalmente a estos datos personales, también es de especial interés la seguridad del resto de información que trata la entidad, como por ejemplo datos de facturación o de clientes, entre otros. Algunos aspectos a considerar en la formación del personal son:

- Aprender a reconocer ataques de ingeniería social, así como a prevenirlos.
- Proteger adecuadamente el puesto de trabajo: uso de antivirus, actualizaciones, etc.
- Poner en práctica controles de acceso físico: dependencias autorizadas, acompañamiento a clientes y proveedores...
- Conocer el manejo de dispositivos

electrónicos.

- Entender los riesgos que puede conllevar el acceso a páginas web externas, descargas o actualizaciones no validadas por el departamento de informática de la corporación.

Otra problemática añadida en este aspecto, es la incesante evolución de la tecnología, lo que inevitablemente obliga a que esta **formación sea continuada y no puntual en el tiempo.**

Además, hay que tener en cuenta que no todo el personal necesita el mismo tipo de conocimientos en materia de seguridad, **adecuando el grado de especialización a cada puesto de trabajo.** Actualmente, en las empresas la mayoría de empleados utiliza dispositivos conectados a los sistemas corporativos, por lo que la seguridad no debe limitarse únicamente a los aspectos técnicos, sino que también debe incorporar aspectos legales y organizativos.

## 2. ESTABLECER POLÍTICAS, NORMATIVAS Y PROCEDIMIENTOS DE SEGURIDAD

Una vez formados los responsables de dirigir las formas de actuar en cada empresa, es necesario elaborar los procedimientos y protocolos de actuación, los cuales deben contar, en líneas generales, con una serie de tareas clasificadas en:

- **Cuestiones técnicas:** alta de un nuevo usuario en el dominio corporativo, acceso a aplicaciones e instalación de estas...
- **Cuestiones administrativas:** firma de un acuerdo de confidencialidad, formación...

Además de documentar todos estos pasos, es preciso especificar lo que se puede y lo que no se puede hacer con los recursos materiales que el empleado tenga a su disposición, relacionados con los **procesos disciplinarios o sanciones** a aplicar en caso de infringir estas normas.



# ¿CÓMO ESTABLECER UNA CULTURA DE SEGURIDAD EN LA EMPRESA?

FUENTE: INCIBE

## 3. SUPERVISAR QUE SE CUMPLEN LAS BUENAS PRÁCTICAS EN SEGURIDAD

Para poder garantizar el cumplimiento de los protocolos establecidos, es necesario que exista un **responsable de seguridad**, que se encargue de velar por:

- **La vigencia y actualización de la normativa y procedimientos** establecidos, atendiendo a posibles cambios de circunstancias o legislación.
- **La implantación de los mismos y su cumplimiento** efectivo por parte del personal de la corporación. Para ello hay que contar con mecanismos que permitan esta supervisión, tales como auditorías internas o externas, incluyendo las auditorías informáticas y base de datos corporativas para avalar la trazabilidad de las operaciones.

Más específicamente, es interesante hablar del **control del uso del correo electrónico**, al tratarse de una herramienta de uso tanto profesional como personal. Esto puede provocar un conflicto entre el derecho de supervisión de la empresa y el derecho de privacidad del empleado. Lo más importante es tener en cuenta que dicha supervisión siempre debe respetar el **principio de proporcionalidad**, controlando la actividad del usuario cuando la organización tiene fundadas sospechas de que éste hace un uso no autorizado del correo. Habitualmente, el conocimiento por parte de los empleados de la existencia de sistemas de monitorización o de un régimen sancionador asociado al incumplimiento de las normas tiene un efecto disuasorio, que también debe formar parte de la cultura de la seguridad.

## 4. REALIZAR ACCIONES DE SENSIBILIZACIÓN Y CONCIENCIACIÓN EN SEGURIDAD PARA LOS EMPLEADOS

Todo lo anteriormente expuesto es necesario, pero no suficiente para crear una cultura de seguridad. Es crucial asegurarse de que todos los empleados estén implicados en este aspecto, y que sean conscientes de la importancia que tiene la información que manejan. **Las campañas de sensibilización y concienciación** son un instrumento fundamental para mantener los niveles de seguridad adecuados, ya que los empleados, no solo son los encargados de cumplir con las normas de seguridad, sino que también son una de las partes más importantes en el mecanismo interno de revisión y mejora en este ámbito.

El objetivo de la empresa debe ser concienciar al

personal sobre su papel en el mantenimiento de la información de la empresa. Como ya se ha comentado, la continua evolución tecnológica conlleva paralelamente el desarrollo de nuevos riesgos asociados, como ocurre con el uso de los BYOD (*Bring Your Own Device*). Esto es, el uso de dispositivos personales del trabajador conectados a la red corporativa para leer su correo electrónico, acceder a aplicaciones, etc. En estos casos, es imprescindible concienciar al personal sobre el riesgo que supone almacenar información confidencial en dispositivos “no controlados”.

Igualmente, de acuerdo con los numerosos avisos que el INCIBE difunde reiteradamente, los trabajadores deben tener conocimientos básicos sobre los frecuentes ataques mediante **ingeniería social** que sufren la mayor parte de usuarios de Internet. A continuación, se enumeran algunos temas sobre los que es conveniente sensibilizar:

- Uso seguro de redes WiFi y correo electrónico
- Prácticas de navegación segura
- Identificación de virus y malware
- Gestión de contraseñas
- Clasificación de la información
- Borrado seguro de información, además de destrucción segura de documentación en papel.
- Uso de USB
- Seguridad en dispositivos móviles
- Uso de programas de mensajería instantánea
- Riesgo de las redes sociales
- Ingeniería Social

Si incrementamos la seguridad de la empresa, mejoramos la imagen de la misma de cara al cliente, lo que evidentemente repercute de forma positiva en el negocio empresarial. **En otras palabras, concienciar en seguridad de la información es rentable para la empresa.**

Enlace al dossier





# PROTOCOLO DE DENUNCIAS IN SITU: PROPUESTA DE AMPLIACIÓN A LAS AGRESIONES A LOS PROFESIONALES SANITARIOS

El fenómeno de las agresiones en ámbito sanitario observado en los últimos años incide negativamente de forma sustancial en el bienestar y seguridad personal de los profesionales de la salud, y además puede repercutir negativamente en la calidad de la esencial asistencia que prestan al conjunto de la sociedad.

Con el fin de implementar nuevas medidas específicas que permitan frenar la evolución de este fenómeno, en el que dos de cada tres casos el autor de la agresión es el propio paciente, y alrededor del 15% son reincidentes, desde la **Oficina del Interlocutor Policial Nacional Sanitario, dependiente de la Unidad Central de Seguridad Privada de la Policía Nacional**, se ha formulado una propuesta a la Secretaría de Estado de Seguridad con la finalidad de ampliar el Protocolo de denuncias “in situ”, con apoyo telemático, para determinados delitos leves, aprobado por la Instrucción núm. 5/2020, de la Secretaría de Estado de Seguridad.

Dicho Protocolo de denuncias “in situ” tiene por objeto el aprovechar las facilidades tecnológicas disponibles para establecer un procedimiento que permita, con apoyo telemático, la presentación de denuncias ante agentes de las Fuerzas y Cuerpos de Seguridad del Estado por la comisión de determinados delitos leves sin necesidad de que sus responsables, empleados o personal de seguridad privada de los establecimientos adheridos deban desplazarse hasta las dependencias policiales para presentarlas.

De procederse a la ampliación del Protocolo, se podría aplicar cuando simultáneamente se cumplan respecto a los presuntos autores criminales o cómplices las circunstancias ya previstas actualmente para los establecimientos comerciales, siendo los mismos:

- Que el/los autor/es se encuentre/n a disposición policial en el centro sanitario.
- Que haya/n sido/s sorprendido/s in fraganti.

Por otro lado, los centros sanitarios deben reunir los requisitos exigidos actualmente a las entidades comerciales y sus establecimientos, esto es:

- Disponer de un departamento de seguridad formalmente constituido.
- Tener contratado un servicio de vigilantes de seguridad privada.

- Estar en disposición de cumplir las condiciones logísticas necesarias para garantizar tanto la correcta conectividad a los entornos web de las Fuerzas y Cuerpos de Seguridad del Estado territorialmente competentes.
- Contar con un lugar que garantice en un marco de privacidad suficiente para ejecutar el resto de obligaciones operativas derivadas.

Para adherirse, una persona con capacidad de representación suficiente para obligarse en su nombre, deberá suscribir un documento de adhesión con la Policía Nacional, con la Guardia Civil o separadamente con ambos, según el Cuerpo territorialmente competente.

Se estima que la implementación del Protocolo de denuncias “in situ” en el ámbito sanitario conseguiría disminuir el número de agresiones a los profesionales sanitarios e, indirectamente, supondría un impulso en la creación de departamentos de seguridad, así como en el establecimiento de medidas de seguridad y en la contratación de vigilantes de seguridad.



# LOS PASADORES DE LAS MENCIONES HONORÍFICAS DEL PERSONAL DE SEGURIDAD PRIVADA

---

La Orden INT/318/2011, de 1 de febrero, sobre personal de seguridad privada, establece en su artículo 36 que, el personal de seguridad privada que sobresalga en el cumplimiento de sus obligaciones, puede ser distinguido con Menciones Honoríficas de las Categorías A y B. Las menciones se otorgan teniendo en cuenta la especial peligrosidad, penosidad, iniciativa profesional o transcendencia social concurrentes en las personas mencionadas.

La misma Orden Ministerial prevé que las menciones honoríficas permiten el uso de un pasador o distintivo específico sobre el uniforme, con el diseño que se determine. El diseño del pasador no podrá confundirse con los de las Fuerzas y Cuerpos de Seguridad ni de las Fuerzas Armadas.

Por ello, desde esta Unidad Central de Seguridad Privada, y al objeto de visibilizar la distinción y reconocimiento otorgado a aquellos profesionales de la seguridad privada a los que se les ha concedido una mención honorífica, se ha elevado una propuesta a la Secretaría de Estado de Seguridad para la creación de un pasador para cada una de las categorías de menciones honoríficas.

En el caso de ser aceptada la propuesta y creados los pasadores, la posesión de las correspondientes menciones honoríficas daría derecho a poder ostentar los correspondientes pasadores sobre el uniforme, pudiéndose portar tantos pasadores como menciones honoríficas se poseyeran.

## MODELOS DE PASADOR PROPUESTOS

- **Mención Honorífica Categoría A:**



- **Mención Honorífica Categoría B:**



# PREGUNTAS FRECUENTES

## ¿Puede reducirse, por condiciones económicas, un servicio de seguridad privada, sin que se revisen las condiciones de seguridad mínimas establecidas por el Jefe o Director de Seguridad?

El artículo 38 de la Ley 5/2014 de 4 de abril, de Seguridad Privada, bajo el título “Prestación de servicios de seguridad privada”, establece en sus apartados 1º y 3º lo siguiente: “1. Los servicios de seguridad privada se prestarán de conformidad con lo dispuesto en esta ley, en particular en sus artículos 8 y 30, y en sus normas de desarrollo, con arreglo a las estipulaciones del contrato, así como, en su caso, con la autorización concedida o declaración responsable presentada. 3. Reglamentariamente se establecerán las condiciones y requisitos para la subcontratación de servicios de seguridad privada.” En este sentido, el artículo 23 del R.D.2364/1994 por el que se aprueba el Reglamento de Seguridad Privada, con el título: “Adecuación de los servicios a los riesgos”, establece que: “Las empresas inscritas y autorizadas para el desarrollo de las actividades a que se refieren los párrafos a), b), c) y d) del artículo 1 de este Reglamento, antes de normalizar la contratación de un servicio de seguridad, deberán determinar bajo su responsabilidad la adecuación del servicio a prestar respecto a la seguridad de las personas y bienes protegidos, así como la del personal de seguridad que haya de prestar el servicio, teniendo en cuenta los riesgos a cubrir, formulando, en consecuencia, por escrito, las indicaciones procedentes”.

Por otro lado, el artículo 96.1 del ya citado Reglamento, determina que: “Los servicios de seguridad se prestarán obligatoriamente bajo la dirección de un jefe de seguridad, en las empresas de seguridad inscritas para todas o alguna de las actividades previstas en el artículo 1.1, párrafos a), b), c) y d) del presente Reglamento, y en las delegaciones o sucursales abiertas de acuerdo con lo dispuesto en el artículo 17.2 de este Reglamento”. El artículo 35.1 de la ya referida Ley 5/2014 de Seguridad Privada, enumera las funciones del Jefe de Seguridad, señalando, entre otras, las de: “realizar el análisis de situaciones de riesgo y la planificación y programación de las actuaciones precisas para la implantación y realización de los servicios de seguridad privada.” Señalar, por último, la necesidad de tener presente lo dispuesto en el artículo 51.3 de la Ley 5/2014 de Seguridad Privada, en cuanto a la posibilidad que tiene el Ministerio del Interior, o en su

caso, el órgano autonómico competente, de poder ordenar a los titulares de establecimientos o instalaciones industriales, comerciales y de servicios y los organizadores de eventos, la adopción de medidas de seguridad que reglamentariamente se establezcan.

Teniendo en cuenta la normativa de seguridad privada de aplicación a la consulta realizada, indicar que, salvo la existencia de obligación de disponer de un número mínimo de vigilantes para la protección de este tipo de instalaciones, por haberlo dispuesto así la Autoridad competente, conforme al criterio, ya expuesto, del artículo 51.3 de la Ley de Seguridad Privada, corresponde al usuario decidir sobre el número de vigilantes de seguridad y los horarios de prestación del servicio, consignándose todo ello en el correspondiente contrato de arrendamiento del servicio de seguridad privada. No obstante lo anterior, a la hora de implantar los servicios de seguridad privada, corresponderá al Jefe de Seguridad de la empresa contratada, o en su caso, al Director de Seguridad de la usuaria de los servicios contratados, el análisis de las situaciones de riesgo, así como la planificación y programación de las actuaciones precisas, teniendo sus indicaciones, en principio, carácter de recomendación para el titular de la instalación, que, como se ha señalado anteriormente, es el responsable de adoptar la decisión final en cuanto al número de personal y horario en la prestación de los servicios.





# PREGUNTAS FRECUENTES

---

## ¿Un vigilante de seguridad con puesto en un hospital, puede realizar purgas de los grifos del centro diariamente?

En virtud del artículo 6.2.d) de la Ley de Seguridad Privada, se establece como actividad compatible la de “comprobación y control del estado y funcionamiento de calderas, bienes e instalaciones en general, en cualquier clase de inmuebles, para garantizar su conservación y funcionamiento”. Por ello, estos servicios y funciones podrán prestarse o realizarse por empresas y personal de seguridad privada, siempre con carácter complementario o accesorio de las funciones de seguridad privada que se realicen y sin que en ningún caso constituyan el objeto principal del servicio que se preste.

## ¿Puede un vigilante de seguridad atender al rescate de personas que puedan quedarse atrapadas en un ascensor dentro de la instalación en la que presta servicio, cuando no se encuentre en las mismas el personal de mantenimiento?

Por parte de esta Unidad, se significa que, conforme a la Ley 5/2014 de Seguridad Privada, en su artículo 32.1.a) corresponde a los vigilantes de seguridad, entre otras, “ejercer la vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto privados como públicos, así como la protección de las personas que puedan encontrarse en los mismos llevando a cabo las comprobaciones, registros y prevenciones necesarias para el cumplimiento su misión”.

Así mismo, en el artículo 6 de la citada Ley, se regulan las actividades compatibles. Concretamente, el punto 2 determina:

*“Quedan también fuera del ámbito de aplicación de esta ley a no ser que impliquen la asunción o realización de servicios o funciones de seguridad privada, y se regirán por las normas sectoriales que les sean de aplicación en cada caso, los siguientes servicios y funciones:*

*Las de información o de control en los accesos a instalaciones comprendiendo el cuidado y custodia de las llaves, la apertura y cierre de puertas, la ayuda en el acceso de personas o vehículos, , el cumplimiento de la normativa interna de los locales donde presten dicho servicio, así como la ejecución de tareas auxiliares o subordinadas de ayuda o socorro, todas ellas realizadas en las puertas o en el interior de inmuebles, locales públicos, aparcamientos, garajes, autopistas, incluyendo sus zonas de peajes, áreas de servicio, mantenimiento y descanso, por porteros, conserjes y demás personal auxiliar análogo”.*

Por lo anteriormente expuesto, desde esta Unidad Central de Seguridad Privada se considera que el auxilio o rescate de personas que se encuentren encerradas en un ascensor, es una función que puede ser desarrollada por vigilantes de seguridad, si bien deberán contar con la formación específica requerida para realizar tales prácticas.



# PREGUNTAS FRECUENTES

## ¿Es obligatorio que la delegación de funciones del jefe de seguridad de una empresa se deba hacer en cada provincia?

Como consideración previa, hay que tener en cuenta que la delegación de las funciones de los jefes de seguridad viene regulada en el art. 35.3 de la Ley 5/2014, de 4 de abril, de Seguridad Privada, que establece: *“El ejercicio de funciones podrá delegarse por los jefes de seguridad en los términos que reglamentariamente se dispongan”*. Así mismo, el artículo 99 del Real Decreto 2364/1994, de 9 de Diciembre, regula la delegación de funciones de los jefes de seguridad de forma que: *“Los jefes de seguridad podrán delegar únicamente el ejercicio de las facultades para autorizar el traslado de armas o la obligación de efectuar personalmente el traslado, y las relativas a comunicación con las Fuerzas y Cuerpos de Seguridad y a subsanación de deficiencias o anomalías, así como las de dirección e inspección del personal y servicios de seguridad privada, lo que requerirá la aprobación de las empresas, y habrá de recaer, donde no hubiera jefe de seguridad delegado, en persona del Servicio o Departamento de Seguridad que reúna análogas condiciones de experiencia y capacidad que ellos; comunicando a las dependencias de las Fuerzas y Cuerpos de Seguridad el alcance de la delegación y la persona o personas de la empresa en quienes recae, con expresión del puesto que ocupa en la propia empresa. Asimismo, deberán comunicar a dichas dependencias cualquier variación que se produzca al respecto, y en su caso la revocación de la delegación”*. A este respecto, el artículo 18 de la Orden INT/318/2011, de 1 de febrero, sobre personal de seguridad privada dice que: *“(…) 2. Lo establecido en el artículo 99 del Reglamento de Seguridad Privada sobre delegación de funciones del jefe de seguridad, será también aplicable al director de seguridad. 3. La delegación de funciones de los jefes y directores de seguridad deberá recaer respectivamente en personas integradas en su empresa o departamento de seguridad. (...) 5. Estas delegaciones de funciones se documentarán mediante solicitud remitida a la Unidad Orgánica Central de Seguridad Privada del Cuerpo Nacional de Policía, que registrará, si procede, la correspondiente aceptación, que deberá exhibir el interesado ante los*

*miembros de los Cuerpos de Seguridad que se lo requieran”*. Con base en lo expuesto, las empresas de seguridad privada deben comunicar a la Unidad Central de Seguridad Privada el alcance de la delegación, así como la persona/s de la mercantil en quienes recae dicha delegación. El “alcance de la delegación” vendría referido a las funciones que podrían ser objeto de delegación, atendiendo al ámbito material, y no respecto al territorial del mismo, que podrían, o no, especificarlo en la solicitud remitida a la UCSP para que procediera a su aceptación.

Con la entrada en vigor de la Ley 5/2014, de 4 de abril, de Seguridad Privada, se modificó la interpretación dada al contenido del artículo 99 del RSP, en el sentido de que el “alcance” va directamente relacionado con las funciones objeto de delegación, y no al ámbito territorial de la misma. No obstante, quien delega podría establecer restricciones, en cuanto a la delegación de funciones, acotando tanto el ámbito material de la delegación funcional como el ámbito territorial sobre el que puede ejercerse la delegación efectuada.



# NOTICIAS

## EL DÍA DE LA SEGURIDAD PRIVADA EN VALENCIA Y EXTREMADURA

El Día de la Seguridad Privada en la provincia de **Valencia**, que estuvo presidido por el Subdelegado del Gobierno, se celebró por primera vez a nivel provincial en lugar de autonómico. Se entregaron 165 menciones honoríficas, con especial reconocimiento a la labor de los vigilantes de seguridad que prestaron servicio en hospitales y centros de salud durante la pandemia.

La comisión organizadora reconoció a la Policía Nacional con la entrega de una placa al Jefe Superior de Policía de Valencia que fue recogida por su Jefe Regional de Operaciones, el cual felicitó a los mencionados por la profesionalidad demostrada, subrayando el papel esencial que la seguridad privada desempeña en nuestra sociedad.



### VALENCIA

En Badajoz, el acto del “**XI Día de la Seguridad Privada de Extremadura**” estuvo presidido por la Delegada del Gobierno en la comunidad, a la que acompañaron el Comisario Provincial de Badajoz y el Jefe de la Unidad Central de Seguridad Privada. Se entregaron 24 menciones honoríficas a personal de seguridad privada y también se reconoció la labor de la Policía Nacional con la entrega de una placa conmemorativa a la Jefatura Superior de Policía de Extremadura que fue recogida por el Comisario Provincial de Badajoz.



### BADAJOZ

## RED AZUL 21: CONTINUAMOS JUNTO A LOS VIGILANTES

La Unidad Central de Seguridad Privada continúa visitando a los vigilantes de seguridad en sus puestos de trabajo, afianzando la relación de los mismos con la Policía Nacional.





# NOTICIAS

## CUARTO CONGRESO DE DERECHO SANITARIO DE LA COMUNIDAD VALENCIANA

Durante los días 30 de septiembre y 1 de octubre se celebró en el Paraninfo de la Universidad CEU Cardenal Herrera en Alfara del Patriarca (Valencia) la cuarta edición del Congreso de Derecho Sanitario de la Comunidad Valenciana organizado por la Asociación de Derecho Sanitario de la Comunidad Valenciana.

Al mismo, acudieron invitados por la organización tanto el Interlocutor Policial Nacional Sanitario junto a un integrante de su Equipo y los Interlocutores Territoriales de Valencia y Alicante.

Entre los diferentes temas que se trataron, cabe destacar por su estrecha relación con las consecuencias de las agresiones a sanitarios la ponencia titulada "Impacto del Covid-19 en los profesionales sanitarios. Afectaciones psicológicas y repercusión laboral."



## EL DÍA DE LA POLICÍA EN CÓRDOBA: RECONOCIMIENTOS AL SECTOR SANITARIO

El pasado día 1 de octubre se celebró el Día de la Policía en Córdoba.

Entre diferentes reconocimientos que se realizaron, especial mención merece el que se hizo al hospital universitario Reina Sofía, al Colegio de Médicos y al Colegio de Enfermería de dicha provincia, de los que hicieron entrega la Subdelegada del Gobierno y el Comisario Provincial de Córdoba, subrayando con ello los méritos por su labor durante la pandemia, así como la estrecha colaboración del sector sanitario con la Policía Nacional a través del Interlocutor Policial Territorial Sanitario.



# NOTICIAS

## LA FORMACIÓN A VIGILANTES DE SEGURIDAD DEL SECTOR SANITARIO SE EXTIENDE A LOS DEL RESTO DE SECTORES

El pasado mes de junio se inició una formación telemática dirigida a los vigilantes de seguridad que prestan servicio en el sector sanitario, la cual ha continuado durante el mes de septiembre.

El contenido de la misma son las técnicas y herramientas de comunicación para gestionar situaciones conflictivas y que las mismas no deriven en violentas.

Estos contenidos fueron elaborados por las expertas del Equipo Nacional del Interlocutor Policial Sanitario de la Policía Nacional encuadrado en la Unidad Central de Seguridad Privada y dirigidos en su inicio a la formación del personal sanitario con el objetivo de disminuir el número de agresiones sufridas por el mismo.

En vista del éxito de la formación impartida a los profesionales de la salud, se decidió extender dicha formación al personal de seguridad que desarrolla su servicio en el ámbito sanitario por ser, en muchas ocasiones, víctimas colaterales de las agresiones que se producen en el ámbito de la atención sanitaria.



En vista de la demanda de los profesionales del sector de la seguridad privada para que dichas técnicas y herramientas de comunicación fueran también dadas a conocer a los vigilantes de seguridad que desarrollan su servicio en otros ámbitos, se decidió abrir dichas jornadas de formación a todos los vigilantes de seguridad y se complementaron los contenidos impartiendo, además, técnicas básicas de autoprotección y de defensa personal policial.

Estas acciones formativas se van a continuar impartiendo para dar respuesta a los requerimientos de los profesionales de la seguridad privada para recibir dicha formación.



## FINALIZACIÓN DE PRÁCTICAS EN LA UCSP DE ALUMNOS DE LA UNIVERSIDAD ANTONIO NEBRIJA



A finales del pasado mes de agosto finalizaron el periodo de prácticas en la Unidad Central de Seguridad Privada cinco alumnos de la Universidad Antonio de Nebrija que se ha llevado a cabo en virtud del "Convenio de Colaboración entre el Ministerio del Interior y la Universidad Antonio Nebrija para el desarrollo de prácticas universitarias", firmado el 19 de agosto de 2019.

Las prácticas han supuesto la culminación de los estudios correspondientes al Máster Universitario en Seguridad y Defensa y al Máster Universitario en Relaciones Internacionales, y han tenido una duración de 250 horas, con un aprovechamiento excelente por parte de todos los alumnos.

Continuando con esta labor de tutorización, a primeros del mes de septiembre se incorporaron tres nuevos alumnos que también realizarán sus prácticas en la Unidad Central.





# NOTICIAS

## POLICÍA NACIONAL DETIENE A UNA ASPIRANTE A VIGILANTE DE SEGURIDAD POR FALSIFICACIÓN DOCUMENTAL DURANTE LAS PRUEBAS SELECTIVAS

Durante el último proceso de selección para vigilante de seguridad, escolta privado y vigilante de explosivos, el Grupo Operativo de Investigación de la Unidad Central de Seguridad Privada detuvo a una aspirante, a la cual se le imputaron dos delitos de falsedad documental.

La aspirante había superado las pruebas selectivas, y en la fase de entrega documental para la acreditación del cumplimiento de los requisitos exigidos en la normativa vigente, presentó dos documentos que levantaron las sospechas de los funcionarios del Área de Procesos Selectivos de la División de Formación y Perfeccionamiento sobre la autenticidad de los mismos, por lo que informaron a la Unidad Central de Seguridad Privada de la Comisaría General de Seguridad Ciudadana.

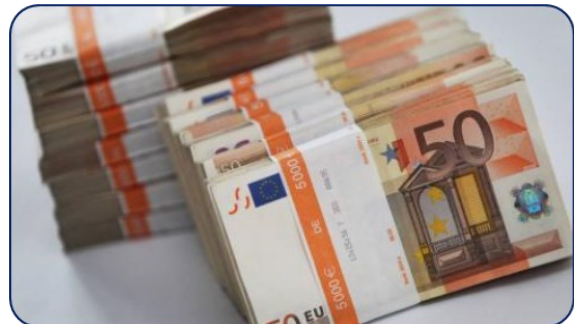
Las gestiones realizadas por el Grupo Operativo de Investigación de la Unidad Central confirmaron la falsedad de la documentación aportada por la aspirante, por lo que se procedió a su detención y puesta en conocimiento de los hechos a la Autoridad Judicial, que abrió un procedimiento para el enjuiciamiento penal de los hechos.



## LA POLICÍA NACIONAL DESARTICULA UN GRUPO CRIMINAL POR UN FRAUDE DE MÁS DE 4.000.000 DE EUROS A LA SEGURIDAD SOCIAL A TRAVÉS DE EMPRESAS DE SEGURIDAD

En una investigación de la Policía Nacional llevada a cabo de forma conjunta entre la Unidad Central de Delincuencia Económica y Fiscal (Comisaría General de Policía Judicial), la Unidad Central de Seguridad Privada (Comisaría General de Seguridad Ciudadana) y la Unidad Territorial de Seguridad Privada de la Comisaría Provincial de Cádiz, se desarticuló un grupo criminal que había defraudado más de 4.000.000 de euros a la Tesorería General de la Seguridad Social mediante un complejo entramado de empresas de seguridad.

El entramado empresarial llevaba a cabo diferentes actuaciones con el objetivo de no abonar las grandes deudas generadas con la Seguridad Social. Utilizaban a personas con escasos conocimientos en la gestión de este tipo de empresas, o familiares desvinculados de los negocios, con el fin de dificultar la identidad del verdadero responsable del pago.



Asimismo se detectaron trabajadores que no estaban dados de alta, exigencia de trabajar más horas que las estipuladas en los contratos, no conceder vacaciones o no pagar los salarios





# NOTICIAS

## LA POLICÍA NACIONAL ALERTA DE UNA MODALIDAD DE FRAUDE BANCARIO MEDIANTE SMS Y LLAMADAS TELEFÓNICAS

La nueva modalidad detectada combina el envío de SMS falsos, que simulan proceder de la entidad bancaria de la que la víctima es cliente, junto con posteriores llamadas de supuestos empleados del banco con el fin de aumentar la credibilidad del engaño.

El SMS que recibe la víctima alerta con el siguiente mensaje: *"Hemos detectado intentos de acceso sospechosos a su cuenta. Debe activar su sistema de seguridad web o bien su cuenta quedará bloqueada"*. Además, incluye un enlace que hace creer al usuario que le reconducirá al acceso a su banca electrónica, cuando en realidad le dirige a una página web falsa donde le solicitan sus datos bancarios. Además, en esa web se advierte que el usuario recibirá una llamada telefónica para realizar las supuestas verificaciones de seguridad.



Cuando los estafadores se ponen en contacto telefónico con las víctimas, las informan de que existen movimientos sospechosos en su cuenta y que para resolverlos necesitan sus claves de firma electrónica. Mientras hablan, y para dar mayor credibilidad al engaño, pueden emitir nuevos SMS informando de las supuestas gestiones. Con este elaborado proceso, los delincuentes consiguen tener acceso total a la banca online de sus víctimas y pueden realizar pagos y transferencias mientras mantienen la comunicación con los estafados.

## LA POLICÍA NACIONAL EN LAS II JORNADAS TÉCNICAS DE SEGURIDAD EN CASINOS Y ESTABLECIMIENTOS DE JUEGO

En el mes de septiembre, se celebró en el Casino Gran Madrid de Torrelodones (Madrid), organizada por CUADERNOS DE SEGURIDAD, la II Jornada Técnica de Seguridad en Casinos y Establecimientos de Juego, contando con la asistencia de integrantes de la Unidad Central de Seguridad Privada de la Policía Nacional.

En el acto participaron ponentes de diferentes áreas relacionadas con el sector, incluida una relacionada con la inteligencia aplicada al ámbito de la seguridad. Además, se trataron temas como la gestión de crisis o la responsabilidad penal de los Directores de Seguridad. Especialmente destacada fue la exposición realizada por la Inspectora de la Policía Nacional Mónica Alba, Jefa de uno de los grupos CENPIDA (Centro Nacional Policial por la Integridad en el Deporte y las Apuestas) del Servicio de Control de Juegos de Azar (Comisaría General de Policía Judicial), que hizo hincapié en cuestiones prácticas vinculadas con la prevención e investigación de los delitos relacionados con el juego.

De las diferentes presentaciones quedó evidenciado la cada vez más habitual e importante figura de la colaboración, no sólo entre el sector de la seguridad privada y las Fuerzas y Cuerpos de Seguridad, sino también entre el propio sector, en este caso, la colaboración y cooperación entre los diferentes departamentos de seguridad que garantizan el buen desenvolvimiento de las actividades lúdicas de los casinos.



# NOTICIAS

## LA POLICÍA NACIONAL EN LA II JORNADA SOBRE CRA'S

El 22 de septiembre se celebró un evento on line sobre el impacto de las tecnologías en la gestión de alarmas: nuevos retos y oportunidades.

En este encuentro, organizado por la revista SEGURITECNIA, se trataron temas tales como el balance de situación de las Centrales Receptoras de Alarmas (CRA) en España, los nuevos entornos tecnológicos y el enfoque de una seguridad integral como requerimiento regulatorio en la Unión Europea, participando profesionales de seguridad privada así como representantes de la seguridad pública de las diferentes Fuerzas y Cuerpos de Seguridad, entre ellos el Jefe de la Unidad Central de Seguridad Privada, el Comisario Principal Manuel Yanguas Menéndez, el cual expuso el papel que representa la colaboración público-privada.

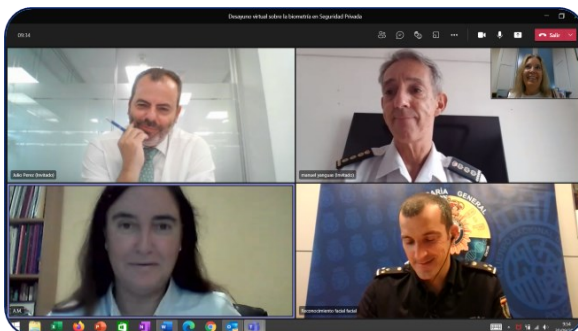


## LA POLICÍA NACIONAL EN EL “DESAYUNO VIRTUAL SOBRE LA BIOMETRÍA EN SEGURIDAD PRIVADA”

El 30 de septiembre se celebró el “Desayuno virtual sobre biometría en seguridad privada”, organizado por la Asociación Española de Empresas de Seguridad (AES).

En el mismo se trataron diferentes cuestiones relacionados con la biometría y su aplicación por los agentes del sector de la seguridad privada como fue la legitimación tecnológica en seguridad privada.

El desayuno contó con la participación del Inspector de la Policía Nacional Sergio Castro del Grupo de Fisonómicos de la Unidad Central de Identificación de la Comisaría General de Policía Científica que explicó la identificación facial en el ámbito de la seguridad privada. El Inspector fue presentado por el Jefe de la Unidad Central de Seguridad Privada.



## EL RECICLAJE DE LOS VIGILANTES DE SEGURIDAD EN 2021: POSIBILIDAD DE REALIZARSE EL 100 % EN MODALIDAD NO PRESENCIAL

El Ministerio del Interior ha publicado en el mes de septiembre la *Orden INT/1019/2021, por la se adoptan medidas excepcionales en materia de formación permanente de los vigilantes de seguridad privada como consecuencia de la situación de crisis sanitaria ocasionada por COVID-19.*

Aún teniendo en cuenta los avances en la lucha contra la pandemia del COVID-19, especialmente tras la puesta en práctica y desarrollo del plan de vacunación, el Ministerio del Interior ha estimado conveniente dispensar, durante 2021, la obligatoriedad de impartir al menos el 50% de la formación de actualización o especialización de forma presencial, pudiendo impartirse en su totalidad en modalidad no presencial.

Tal y como dice la citada Orden : *“Durante el 2021, los cursos anuales de actualización o especialización para los vigilantes de seguridad a los que se refiere el artículo 57 del Reglamento de Seguridad Privada, aprobada por el Real Decreto 2364/1994, de 9 de diciembre, y el artículo 7 de la Orden INT/318/2011, de 1 de febrero, sobre personal de seguridad privada, podrán realizarse en su totalidad de forma no presencial.”*

Esta medida, de carácter excepcional, no es aplicable a la formación específica a la que se refiere el artículo 8 de la Orden INT/318/2011.

