# BOLETÍN R@S

NÚMERO 29 JULIO 2023

UNIDAD CENTRAL DE SEGURIDAD PRIVADA

## C1B3RWALL
### UNO DE LOS EVENTOS FORMATIVOS DE CIBERSEGURIDAD MÁS IMPORTANTES DEL MUNDO

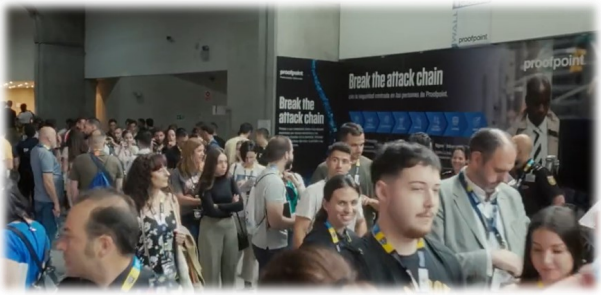
# C1B3RWALL: CONGRESO DE SEGURIDAD DIGITAL Y CIBERINTELIGENCIA

La Escuela Nacional de Policía (Ávila) acogió los días 20, 21 y 22 de junio la III edición del Congreso de Seguridad Digital y Ciberinteligencia-C1b3rWall– bajo el título *"Futuro Inmersivo"*



**Más de 200 ponentes, tanto nacionales como internacionales**

**+6800 INSCRITOS**




**MÁS DE 100.000 INSCRITOS ONLINE PROCEDENTES DE MÁS DE 82 PAÍSES**

**UN ESCAPARATE DE ALCANCE INTERNACIONAL.**

**EL CONGRESO DE CIBERSEGURIDAD CON MÁS PARTICIPANTES DE ESPAÑA**

# C1B3RWALL: CONGRESO DE SEGURIDAD DIGITAL Y CIBERINTELIGENCIA

## STANDS Y ACTIVIDADES



**Exhibiciones de Guías Caninos, Caballería, Tedax y Medios Aéreos, entre otras especialidades**

**El Ministro del Interior, acompañado del Director General de la Policía, clausuró la III edición de C1b3rWall**


Para conocer más detalles PINCHA AQUÍ

200 1824 · 2024 POLICÍA NACIONAL

# LA VENTANA DEL R@S: LA LUCHA DE LALIGA CONTRA LA VIOLENCIA EN EL DEPORTE

## Dirección de Integridad y Seguridad de la LaLiga.

La discriminación racial es un problema presente en todos los ámbitos de la sociedad. Los acontecimientos ocurridos últimamente en algunos estadios de futbol españoles han hecho que se eleve el debate sobre este tema. La Dirección de Integridad y Seguridad de **LaLiga** lleva años estudiando y tomando medidas recogidas en informes para poder hacer frente a la **lucha contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.**

Este órgano, dentro de sus competencias, lleva tiempo desarrollando múltiples acciones, siendo las más importantes las denuncias ante la Justicia y ante la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte (**CEVRXID**).

Es por ello por lo que las Direcciones de Integridad y Seguridad y de Legal de LaLiga denuncian de forma contundente cualquier tipo de violencia ocurrida dentro y fuera de los estadios de fútbol profesional desde hace varias temporadas. Lo que se pretende con estas medidas es la **violencia cero en el deporte**, y para ello se llevan a cabo diferentes prácticas de prevención, detección y denuncia en cada jornada, que son trasladadas a la CEVRXID, así como al Comité de Competición de la Real Federación Española de Fútbol (RFEF). Del mismo modo, este órgano denuncia y se persona como acusación en cualquier procedimiento penal relacionado con hechos violentos ocurridos en el ámbito del fútbol.

Para acelerar la identificación de cualquier persona o grupo de personas que manifiesten conductas racistas en cualquier estadio o fuera de él, han habilitado durante la temporada 22/23 varios canales de denuncia, para que los aficionados puedan ponerse en contacto con este departamento y facilitar la identificación necesaria en relación con ellas.

### CANALES DE DENUNCIA

**StopRacismo@laliga.es**
**Telegram @StopRacismoLaLiga**

En cuanto a la actuación en este tipo de conductas, LaLiga solo puede denunciar los hechos, ya que la regulación aplicable en España para la imposición de sanciones por conductas racistas es la recogida en la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.

En el caso de posibles sanciones administrativas, su artículo 28 atribuye la competencia sancionadora a la Delegación del Gobierno, la Secretaría de Estado de Seguridad, el Ministerio del Interior y el Consejo de Ministros, sin perjuicio de las posibles competencias de las Comunidades Autónomas. Por tanto, LaLiga solo puede limitarse a denunciar los hechos, que es lo que hace.

En cuanto a las sanciones disciplinarias deportivas, éstas vienen recogidas en el Código Disciplinario de la Real Federación Española de Fútbol, que incorpora las infracciones previstas en los artículos 34 y sig. de la Ley 19/2007, de 11 de julio, siendo competente para su sanción el Comité de Competición.

### DIRECCIÓN DE INTEGRIDAD Y SEGURIDAD DE LALIGA

Desde la creación de la Dirección de Seguridad de LaLiga (temporada 14/15), con posterioridad Dirección de Integridad y Seguridad (15/16), se han implementado distintas acciones en el marco de un plan estratégico ideado desde esa Dirección con la intención de cumplir con el compromiso adquirido por el actual presidente y que afianzan la posición de LaLiga en su afán por combatir y erradicar este tipo de comportamientos.

Dentro de la Dirección de Integridad y Seguridad se encuadra la Unidad de Análisis de Seguridad. Su cometido es la realización de estudios, análisis e investigaciones relacionadas con la prevención de la violencia, el racismo, la xenofobia y la intolerancia, y cuyas conclusiones son difundidas a distintos organismos (clubs, Policía Nacional, y la Comisión).

Entre otras acciones, desde esta Dirección se difunden semanalmente informes sobre la previsión de actividad de los grupos de aficionados de riesgo (ultras) para cada jornada de liga y se realiza una valoración de riesgo de todos los partidos. En caso de considerarse necesario se traslada la información a los clubes implicados.

Igualmente, se realizan informes de valoración de riesgo en partidos de competición europea cuando los clubes de LaLiga disputan dichos encuentros en territorio nacional.

Estos informes se envían a los clubes para facilitar información sobre los aficionados extranjeros en previsión de su desplazamiento a España con el fin de prevenir posibles acciones violentas y aportar información que pueda ser de utilidad a la hora de elaborar el dispositivo de seguridad.

Esta Unidad ha elaborado un protocolo de actuación en materia de lucha contra la violencia, racismo, xenofobia e intolerancia en el deporte. Este plan de actuación se divide en dos partes: **prevención y denuncia**.

## PREVENCIÓN

Una de las actuaciones que realiza LaLiga para luchar contra estos hechos delictivos es la **comunicación/ concienciación.**

Se trabaja en una máxima: **tolerancia cero con cualquier tipo de discriminación**, ya sea por raza, nacionalidad, religión, lengua, sexualidad o discapacidad. Cualquier comportamiento que atente contra los valores de igualdad que deben imperar en el deporte se expone a ser denunciado ante los organismos deportivos o jurídicos competentes.

Para ayudar a dar a conocer esta máxima, se elabora y difunde el **"manual del aficionado".** Realizado por LaLiga y Aficiones Unidas, este manual pretende ser la guía de referencia para los aficionados al fútbol. Su objetivo es resaltar los valores positivos del deporte, difundir una imagen de concordia y fomentar el espíritu de juego limpio en el fútbol profesional español. Este manual, que se repartió durante varias temporadas en los accesos a los estadios, está disponible en formato digital en la microsite de Aficiones Unidas dentro de la página web de LaLiga.

PINCHA PARA DESCARGARLO

Igualmente, se facilita a los clubes cartelería, en la que, en cumplimiento con la normativa de antiviolencia vigente, se especifican las condiciones de acceso y permanencia en los estadios. Están visibles en los accesos y en distintas zonas de la instalación deportiva.

Otra actuación importante de LaLiga es la **formación**. Desde la Dirección de Integridad y Seguridad se organiza y participa en distintas actividades de carácter formativo, entre las que se encuentran:

- **Comité de seguridad.** Dirigido a los directores de seguridad de los clubes, donde se unifican criterios y estrechan relaciones entre los representantes de los clubes.
- **Seminario de seguridad.** En el que participa Policía Nacional, los directores de seguridad de los clubes y representantes de las federaciones de peñas de aficionados (AFEPE), que busca mejorar la coordinación entre los distintos actores.
- **Curso de seguridad en eventos deportivos:** Organizado por la Business School, donde miembros de esta Dirección exponen las diversas acciones desarrolladas en la lucha contra la violencia, el racismo y la intolerancia en el deporte.


- **Jornadas formativas dirigidas a vigilantes de seguridad,** organizadas en colaboración con la Policía Nacional, dirigidas a los vigilantes de seguridad que prestan servicios en los estadios de fútbol. Se imparten contenidos sobre delitos de odio y asistencia de personas con discapacidad a eventos deportivos con el fin de lograr su plena inclusión. También, se exponen las condiciones de acceso a los estadios, safety y las acciones que realiza LaLiga contra los grupos de riesgo (ultras).

- **Otras actividades formativas.** Colaboraciones habituales de miembros de esta Dirección con distintas organizaciones (LaLiga Work, curso de coordinadores de seguridad de Policía Nacional., Policía Local de Villarreal, EDF, CEPOL, AFE, ADSI)

## DENUNCIA

Entre sus compromisos mas importantes está la presentación de **informes/denuncia** contra todos estos comportamientos violentos, racistas, xenófobos o intolerantes ocurridos con motivo de partidos de fútbol, personándose como acusación particular siempre que se produce algún hecho de esta etiología. Se han constatado más de una docena de incidentes/acciones racistas vinculados a partidos de LaLiga. Todos los casos han sido investigados y/o denunciados ante los organismos e instancias competentes. Algunos de estos episodios se produjeron dentro del campo. En estas ocasiones, se analizan los audios y archivos digitales, así como informes periciales externos con el análisis de lectura de labios, para aportar toda esta información a las instancias en las que presentamos sus denuncias.

Este compromiso se articula en dos acciones:

- **Representación** de LaLiga en la **CEVRXID,** aportando a este organismo todas las denuncias por cánticos racistas xenófobos o que incitan a la violencia ocurridos con motivos de partidos de LaLiga, así como invasiones de campo y lanzamientos de objetos. Igualmente, se presentan denuncias de estas actuaciones ante el Comité de Competición de la RFEF y se hace seguimiento de los expedientes sancionadores.

- **Personaciones judiciales.** Se elaboran informes que ayudan a sustentar la personación de esta dirección en los distintos procedimientos relacionados con la violencia, el racismo, la xenofobia y la intolerancia en el deporte y en los que LaLiga se persona como acusación particular. De igual forma, miembros de la Dirección asisten como peritos en procedimientos judiciales relacionados con conductas violentas denunciadas por LaLiga.

## OTRAS ACCIONES

- **Manual del Jugador**: Se entrega cada inicio de temporada a todos los jugadores, tanto en formato físico como a través de la App Players exclusiva de jugadores. En él se conciencia a los jugadores sobre la violencia y el racismo y se les anima, no solo a vivir los valores del respeto, sino también a denunciar las conductas violentas o racistas.
- **Proyectos en colaboración con los clubes**: mensajes contra el racismo y la xenofobia en la megafonía y videomarcadores de los estadios y en sus redes sociales.


- **Colaboración institucional de LaLiga**. Reuniones con el Ministerio de Igualdad y con el Ministerio de Derechos Sociales y Agenda 2030, a cuyos gabinetes se informa puntualmente de las acciones que llevan a cabo desde este organismo en materia de denuncias y lucha contra el racismo. Recientemente se presentó una campaña de concienciación respecto del racismo en el deporte, para realizar de forma conjunta.

**Con la aproximación del plazo marcado por la Orden INT/826/2020, de 3 de septiembre, por la que se modifican, en lo relativo a plazos de adecuación de medidas de seguridad electrónica, la Orden INT/314/2011, de 1 de febrero, sobre empresas de seguridad privada, la Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, y la Orden INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada, todo ello para la adecuación de los sistemas de seguridad electrónica, parece acertado realizar una valoración de diferentes aspectos que pudieran afectar a las empresas de seguridad, así como a los usuarios de sus servicios**

### 1.- Aspectos que deben ser tenidos en cuenta:

Dicha Orden Ministerial modifica los plazos de adecuación señalados, en su momento, por las ya mencionadas Órdenes Ministeriales 314, 316 y 317 del año 2011, fijando como último día para poder llevar a cabo esas actualizaciones de los sistemas de seguridad electrónica, el día 31 de diciembre de 2023.

Siendo así que la Disposición transitoria primera de la Orden INT/316/2011, relativa a la "Adecuación de sistemas ya instalados", una vez operada esa modificación, quedo definida, en su párrafo primero, de la siguiente forma:

*"Los sistemas de seguridad instalados y conectados a centrales de alarmas o a centros de control, antes de la fecha de entrada en vigor de esta orden, en establecimientos obligados y no obligados, tendrán de plazo para adecuarse a lo dispuesto en los artículos 2 y 3 de esta orden hasta el 31 de diciembre de 2023".*

Ello supone que el día 1 de enero de 2024, cualquier sistema de seguridad electrónica que se encuentre conectado a una CRA o a un centro de control, debería cumplir con lo dispuesto por, entre otros preceptos, el artículo 2 de la Orden INT/316/2011, respecto a los grados de los sistemas de seguridad, toda vez que establece lo siguiente:

**1.1.- La Norma UNE-EN 50131-1 establece cuatro grados de seguridad** en función del riesgo, quedando en esta Orden asignados, además, en virtud de la naturaleza y características del lugar en el que se va a efectuar la instalación y de la obligación, o no, de estar conectados a una central de alarmas o centro de control, del modo siguiente:

***a) Grado 1,*** *o de bajo riesgo, para sistemas de alarma dotados de señalización acústica, que no se vayan a conectar a una central de alarmas o a un centro de control.*

***b) Grado 2,*** *de riesgo bajo a medio, dedicado a viviendas y pequeños establecimientos, comercios e industrias en general, que pretendan conectarse a una central de alarmas o, en su caso, a un centro de control.*

***c) Grado 3,*** *de riesgo medio/alto, destinado a establecimientos obligados a disponer de medidas de seguridad, así como otras instalaciones comerciales o industriales a las que por su actividad u otras circunstancias se les exija disponer de conexión a central de alarmas o, en su caso, a un centro de control.*

***d) Grado 4,*** *considerado de alto riesgo, reservado a las denominadas infraestructuras críticas, instalaciones militares, establecimientos que almacenen material explosivo reglamentado, y empresas de seguridad de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos, requeridas, o no, de conexión con central de alarmas o, en su caso, a centros de control.*

**1.2.- Los grados exigidos en esta Orden para los sistemas de seguridad quedaran sujetos a lo establecido en la Disposición transitoria segunda de esta Orden.** A su vez, se deberá disponer, para cada uno de los elementos de seguridad instalados, en base a esa adecuación, del certificado de producto que, emitido por el correspondiente ente certificador, acredite disponer del grado de seguridad exigido.

**2.- Los sistemas de seguridad deberían ser adaptados, teniendo en cuenta lo siguiente.**

**2.1.- Sistemas de seguridad ordinarios** (domicilios, mercantiles, entidades comerciales, industriales, etc.) conectados a una central receptora de alarmas o centro de control, habrían de disponer:

- De elementos de seguridad electrónica de Grado 2.
- De un nuevo certificado de instalación, en su caso, que acredite el Grado 2 del sistema de seguridad.
- De un nuevo certificado de conexión, en el caso de estar conectado el sistema a una CRA, todo ello, al verse afectado el propio sistema por los cambios operados en el mismo.

**2.2.- Sistemas de seguridad específicos de establecimientos obligados a disponer de medidas de seguridad electrónica** (se debe tener en cuenta que existen establecimientos que no están obligados a disponer de sistemas de seguridad electrónica) que, conectados de modo ordinario a una CRA, o de modo excepcional a un centro de control, habrían de cumplir con:

- Disponer, en su totalidad, de elementos de seguridad electrónica de Grado 3.
- Emitirse, en su caso, por la empresa de seguridad correspondiente, el certificado de instalación que acredite, precisamente, ser un sistema de Grado 3.

- A su vez, parece acertado recordar que los establecimientos que están obligados a disponer de una unidad de almacenamiento de seguridad, de las reguladas por la Norma UNE-EN 1143-1 (cajas fuertes o cámaras acorazadas), además de conectar su sistema de alarmas a una empresa de seguridad autorizada para la actividad de central de alarmas o, en su caso, a una central, también autorizada, de uso propio, dicha instalaciones, habrían de contar, entre sus elementos, con un sistema de registro de imágenes, de forma que puedan ser utilizados como elemento de verificación por la central de alarmas a la que estuvieran conectados.
- En caso de conexión a CRA, se debería dispone de un nuevo certificado de conexión emitido por la CRA, que acredite la correcta conexión, una vez llevadas a cabo las modificaciones relacionadas con la adecuación del sistema (ha de señalarse que, en el caso de tener conectados a la CRA un sistema no adecuado, este hecho podría ser considerado como la conexión de un sistema de seguridad **NO HOMOLOGADO**).

**2.3.- Sistemas de seguridad electrónica de las empresas de seguridad**: En cuanto a las medidas de seguridad electrónica de sus sedes o delegaciones, éstas deberían adaptarse a lo señalado por la modificación operada en el apartado 2 de la Disposición Transitoria Única de la Orden INT/314/2011, por la Orden INT/826/2020, en cuanto a que: *"Las medidas de seguridad electrónica y los sistemas de alarma instalados en las empresas de seguridad antes de la fecha de entrada en vigor de esta orden tendrán de plazo para adecuarse a lo dispuesto en la misma hasta el 31 de diciembre de 2023.»*, de modo que habrían de cumplir con lo siguiente:

- Los elementos de seguridad electrónica habrían de ser, en general de Grado 3, salvo las empresas de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos, cuyo Grado habrá de ser 4.
- Todo debería estar acreditado, mediante certificado de instalación, emitido por una empresa de seguridad, respecto que el sistema de seguridad es de Grado exigido y se dispone de doble vía de comunicación con la CRA.
- De igual forma, se debería disponer de un nuevo certificado de conexión, que acredite el buen funcionamiento de la misma (conexión) con la CRA, una vez operada las correspondientes adecuaciones del sistema.
- Cabe recordar, a su vez, que habrán de disponer de doble vía de comunicación con la CRA.

**2.4.- Sistemas de seguridad de infraestructuras especiales,** tales como:

- Infraestructuras críticas.
- Instalaciones militares.
- Establecimientos que almacenen material explosivo reglamentado.
- Empresas de seguridad de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos.

## Todas ellas deberían:

- **Disponer de elementos de Grado 4 en su sistema de seguridad electrónico**, al menos, en todos aquellos casos que se puedan disponer de los mismos, al existir la correspondiente comercialización en el mercado actual. Para lo que habría de tenerse en cuenta lo descrito por el segundo párrafo de la Disposición transitoria primera de la Orden INT/316/2011, relativa a la *"Adecuación de sistemas ya instalados"*, que contempla lo siguiente:

  *"Cuando un sistema de seguridad necesite utilizar componentes que, en el momento de su instalación, no estén disponibles en el mercado, según las normas recogidas en el apartado primero del artículo 3 de esta Orden, se permitirá su conexión, siempre que tales elementos no influyan negativamente en su funcionamiento operativo.*

  *La permanencia de tales elementos en el sistema estará condicionada a la posible aparición de la especificación técnica que lo regule y a su disponibilidad en el mercado.*

  Transcurrido el período de carencia de diez años establecido en el párrafo anterior, se deberá disponer del pertinente certificado emitido por un Organismo de Control acreditado en base a la Norma EN 45011, responsable de la evaluación de la conformidad de los productos y exhibirse en caso de ser requerido".

- **Disponer de un certificado de instalación** emitido por una empresa de seguridad, que acredite esa situación.

- De igual forma, se debería **disponer de un nuevo certificado de conexión**, en su caso, que acredite el buen funcionamiento de la misma con la CRA, una vez operada las correspondientes adecuaciones del sistema.

### 3.- Obligaciones de las empresas de seguridad, según la Ley 5/2014, de Seguridad Privada.

Las empresas de seguridad deben cumplir el principio rector definido por el artículo 8.1 de la mencionada Ley, que establece: *"1. Los servicios y funciones de seguridad privada se prestarán con respeto a la Constitución, a lo dispuesto en esta ley, especialmente en lo referente a los principios de actuación establecidos en el artículo 30, y al resto del ordenamiento jurídico".*

Lo que conlleva que las mismas han de cumplir con la exigencia de adecuar los sistemas de seguridad, que afectan o intervienen en la prestación de los servicios de seguridad que desarrollan.

Así mismo, dicho texto legal contempla como prohibiciones que afectan a las empresas de seguridad, las descritas en su punto 1, apartados c) y d), que se corresponden con:

*" c) La prestación de servicios de seguridad privada incumpliendo los requisitos o condiciones legales de prestación de los mismos."*

*d) El empleo o utilización, en servicios de seguridad privada, de medios o medidas de seguridad no homologadas cuando sea preceptivo, o de medidas o medios personales, materiales o técnicos de forma tal que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones, o cuando incumplan las condiciones o requisitos establecidos en esta ley y en su normativa de desarrollo".*

De tal forma que las empresas de seguridad no podrían prestar servicios de seguridad, en los que suponga incumplir los requisitos y condiciones dispuestos por la normativa para su prestación, como ocurriría en el caso de conectar sistemas de seguridad a una CRA, sin que los mismos se ajusten a los requisitos fijados por la normativa.

Por su parte, el texto legal de 2014, al regular los servicios de instalación y mantenimiento, establece en su artículo 46.1, lo siguiente:

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

A este respecto, cabe entender que las características técnicas determinadas reglamentariamente de los sistemas de seguridad, son las dispuestas, expresamente, por las Órdenes Ministeriales 314, 316 y 317.

En cuanto a la homologación de sistemas de seguridad y su posible conexión a una central receptora de alarmas, el artículo 23 de la Orden INT/314/2011, contempla lo siguiente:

*"Cuando la instalación se conecte a central de alarmas, deberá ajustarse a lo dispuesto en los artículos 40, 42 y 43 del Reglamento de Seguridad Privada, considerándose homologados si reúnen las características determinadas en los artículos 22 y 24 dela presente Orden".*

De tal forma que no parece pueda conectarse a una CRA, un sistema de seguridad que no cumple con lo establecido en dicho precepto, donde se exige el cumplimiento de la norma UNE EN 50131, que precisamente establece los grados de seguridad que deben cumplir los sistemas de seguridad de usuarios, establecimientos obligados, etc.

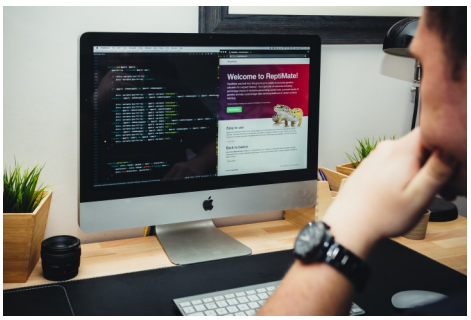
## 4.- Posibles infracciones:

### 4.1- Para las empresas de seguridad:

- Cuando no adapten los sistemas de seguridad de sus sedes o delegaciones a lo exigido en la normativa, en tanto supone no adoptar medidas de seguridad de carácter obligatorio.

  Artículo 57.1.j), de la LSP, que considera como infracción de carácter grave: *"La ausencia de las medidas de seguridad obligatorias, por parte de las empresas de seguridad privada y los despachos de detectives, en sus sedes, delegacio*nes y sucursales".

- Empresas de seguridad que realizarán la instalación de medios materiales no homologados, cuando la homologación es preceptiva, no instalando el grado de seguridad exigido. Artículo 57.2.a) de la LSP, que considera como infracción de carácter grave: *"La instalación o utilización de medios materiales o técnicos no homologados, cuando la homologación sea preceptiva",* en base al no cumplimiento de lo señalado por el articulo 23 de el artículo 23 de la Orden INT/314/2011, de empresas de seguridad.



- Empresa de CRA que tiene conectados a su central sistemas de seguridad de usuarios que no disponen del grado de seguridad exigido, haciendo uso o utilización de esos medios en la prestación del servicio. Artículo 57.2.a) de la LSP, que considera como infracción de carácter grave: "*La instalación o utilización de medios materiales o técnicos no homologados, cuando la homologación sea preceptiva",* toda vez que parece que se utilicen, en las actuaciones de recepción de las señales de alarmas, elementos que no se encuentran debidamente homologados, en virtud de lo dispuesto por el artículo 23 de la Orden INT/314/2011, de empresas de seguridad.

**4.2- Usuarios de sistemas de seguridad:**

- Establecimientos obligados a disponer de medidas de seguridad:

  Artículo 59.1.f) de la LSP, que considera como infracción de carácter muy grave: *"La falta de adopción o instalación de las medidas de seguridad que resulten obligatorias",* (pudiendo ser considera como falta de medidas de seguridad de carácter obligatorio, la disposición de aquéllas medidas o elementos que no se ajustan a lo señalado por la normativa).

- Otras infracciones para usuarios de sistemas de seguridad. Artículo 59.2.b) de la LSP, que considera infracción de carácter grave, la relativa a:

  *"La utilización de aparatos de alarma u otros dispositivos de seguridad no homologados".*

  Toda vez que el usuario hace uso de ese tipo de elementos de seguridad, no homologado, atendiendo a la definición que realiza el artículo 2.13 de la LSP de "elemento homologado".

  *Artículo 59.3. a) de la LSP, que considera como infracción leve: "La utilización de aparatos o dispositivos de seguridad sin ajustarse a las normas que los regulen, o cuando su funcionamiento cause daños o molestias desproporcionados a terceros".*

**5.- Posibilidad de tramitar la baja de aquellos contratos de clientes (usuarios), que no acepten adecuar su sistema de seguridad al grado exigido por la normativa.**

No parece desacertado que las empresas de seguridad (especialmente las que disponen de contratos de conexión de sistemas de seguridad a CRA o a centros de control o de videovigilancia), para aquellos casos que los clientes no se adecúen al grado exigido por la normativa, puedan gestionar la posible rescisión del contrato del servicio de seguridad, y como tal, comunicar la baja del mismo al Ministerio del Interior, al no adaptar sus sistemas a lo exigido por la normativa.

## SIMULACIÓN POLICIAS EN DELITOS ON LINE

Se trata de una campaña de extorsión, en la cual **los ciberdelincuentes suplantan la identidad de Fuerzas y Cuerpos de Seguridad del Estado**, acusando a las víctimas a través de un correo, indicando que ha visitado sitios web de pornografía infantil y que ha cometido otros delitos relacionados con este. En un documento adjunto indican que tiene un plazo comprendido entre 24 o 72 horas, en el cual se exige enviar al correo proporcionado una serie de datos para justificar dichas acusaciones. En caso de no hacerlo, procederán a ejercer cargos penales contra la víctima.

El correo malicioso se envía a través de una cuenta de correo aleatoria que no guarda relación con las instituciones suplantadas.

Otro detalle de estos correos es que están escritos de forma alarmante y con faltas de ortografía.

Los estafadores piden a la víctima que se responda al correo en un plazo de 24-72 horas. y en caso de no recibir justificación se procederá a sancionarla.

### SOLUCIÓN

En caso de haber recibido el correo mencionado **marca dicho correo como spam y elimínalo.**

En caso de haber enviado el correo solicitado por el ciberdelincuente proporcionando tus datos **acude a denunciar los hechos ante la Policía Nacional.**

## MAN IN THE MIDDLE

Traducido del inglés al castellano significa «hombre en el medio». Destaca por la cantidad de información a la que pueden llegar a acceder en caso de que tengan éxito.

El delincuente intercepta la comunicación entre dos o más personas y suplanta la identidad de alguno de ellos para consultar información y modificarla a conveniencia. Para ello emplea diversas técnicas que complican la detección, utilizando puntos de acceso wifi públicos o con bajo nivel de seguridad, en el que el ciberdelincuente permite de forma deliberada la conexión para poder llevar a cabo la estafa. También suelen imitar el nombre de una red cercana (SSID) para crear confusión y que algunas personas se conecten por error.

Las redes locales (Local Area Network LAN) de las empresas también son diana de este tipo de ataques. Concretamente, el ciberdelincuente lanza un ataque en el que engaña a los equipos de la red local haciéndoles creer que es un dispositivo legítimo y fuerza que todo pase a través del dispositivo controlado por el delincuente.

### CONSEJOS PARA EVITAR EL CIBERATAQUE

La prevención es clave para evitar este tipo de estafas. Se recomienda acceder a sitios web seguros, y comprobar que el certificado corresponde a la compañía en cuestión. Asimismo, proteger la red wifi de las empresas, emplear software de seguridad con antivirus y antimalware y mantenerlo actualizado.

## FRAUDE DE TRIANGULACIÓN

El fraude de triangulación ocurre cuando un estafador/ vendedor crea listados en una plataforma o mercado de terceros para artículos que en realidad no tiene en su poder.

El comprador del artículo ve en ese listado, generalmente a un precio demasiado bajo, y compra el artículo. El estafador/vendedor va a un sitio web de comercio electrónico legítimo que vende ese artículo, hace un pedido para enviarlo al comprador desprevenido, utilizando para el pago los datos de una tarjeta de crédito robada, y así realiza esa transacción.

La web de comercio electrónico envía el pedido, y no se da cuenta de que era un fraude hasta semanas después, cuando reciben un contracargo del titular real de la tarjeta de crédito.

El comprador recibe el artículo que compró sin saberlo, y el comerciante legítimo se queda con el pago de una tarjeta fraudulenta, lo que provoca a todos muchos problemas.

Las consecuencias para los comerciantes son las devoluciones de cargo, incluso si el titular de la tarjeta recibió lo que pagó, ya que la compra se realizó sin su autorización y las devoluciones de cargo conllevan tarifas costosas, involucran muchas compras pequeñas e individuales y eso significa que un solo comerciante puede terminar con una gran cantidad de devoluciones de cargo que conlleva unos gastos.

## HUELLA DIGITAL: COMO EVITAR QUE AFECTE A NUESTRAS EMPRESAS.

Ante el gran auge de la digitalización, es importante saber y concienciarse de qué información hacemos pública, ya que si no se trata correctamente, puede tener graves consecuencias para nuestras empresas.

Para saber más sobre la huella digital debemos conocer dos de los métodos de obtención de información más comunes, que son el **footprinting** y **fingerprinting**.

Antes de conocer como funcionan estos dos métodos es necesario saber que son los **metadatos**. Por ejemplo, cuando hacemos una foto con nuestro móvil, el dispositivo guarda información adicional como: la fecha en la que se realizó, el modelo del dispositivo, las coordenadas desde donde se realizó dicha foto, etc.

Esto sucede con multitud de archivos, como los PDF, DOCX, XLSX… Si subimos, por ejemplo, un dosier de un producto, es posible que estemos guardando información como el modelo del ordenador con el que se ha realizado, el nombre del usuario o incluso, contraseñas.

***No ser conscientes de los datos que se comparten en Internet, puede poner en riesgo la seguridad de la empresa, ya que puede dar pie a que los ciberdelincuentes ataquen a los sistemas, redes, ordenadores, etc.***

**¿Qué es el footprinting?**

Es una técnica que consiste en acceder a toda la información pública que la empresa objetivo ha compartido en Internet. Para ello, se miran redes sociales, medios de comunicación o incluso, posibles metadatos de archivos.

Las empresas en su día a día comparten información de forma pública de forma consciente y sin ninguna intención, pero que los ciberdelincuentes aprovechan para llevar a cabo una fase de recopilación de todos esos datos **sin infringir ninguna ley.**

**¿Qué es el fingerprinting?**

También conocida como **"huella digital",** es una técnica que consiste en recopilar información pero que requiere de la interacción con el sistema analizado, pudiendo obtener información sobre el navegador web, el sistema operativo y otras características de un dispositivo para crear un perfil completo del objetivo.

A través de esta técnica, se consigue rastrear a los usuarios para reunir información sobre su comportamiento en Internet sin su consentimiento explícito. Esta información podría utilizarse, por ejemplo, para encontrar un método de acceso a un sistema.

## FUENTE: INCIBE


### HUELLA DIGITAL

### ¿CÓMO PODEMOS EVITAR QUE RECOPILEN INFORMACIÓN SENSIBLE DE NUESTRA EMPRESA A TRAVÉS DE ESTA TÉCNICA?

En primer lugar, debemos ser conscientes de que no podremos eliminar nuestra huella digital en su totalidad, ya que es inevitable dejar rastro en Internet o que algún metadato se comparta sin querer. Sin embargo, se puede reducir considerablemente si se siguen una serie de hábitos y se adquieren unos conocimientos básicos.

En la actualidad, muchas aplicaciones de mensajería y redes sociales eliminan los metadatos al subir imágenes a la red, pero, aun así, hay que tener en cuenta lo que se comparte. No se recomienda subir imágenes de lugares fácilmente identificables o de localizaciones importantes de la empresa (salas de servidores, accesos de seguridad, accesos de emergencia…).

También es importante concienciar a los trabajadores de que no deben hacer fotos en su puesto de trabajo, y menos con la pantalla encendida, ya que podría mostrar información sensible en ella o en la propia mesa de escritorio.

En cuanto a los datos de los documentos, existen herramientas que los eliminan y emplearlas debería ser una práctica habitual a la hora de subir archivos a la Red, ya que evitará posibles fugas de información.

Se deberían utilizar navegadores que tengan opciones de configuración que minimicen el rastro digital, utilizar una VPN también puede ser útil para mejorar la privacidad en línea y reducir la huella digital. Cuando nos conectamos a través de una VPN, la información que se transmite está protegida, por lo que es más difícil saber quién se está conectando a una página web y desde qué dispositivo. Si además se combina una VPN con un navegador que limite el fingerprinting se logrará reducir aún más la huella digital y proteger la seguridad en línea.

La concienciación de los empleados también es fundamental en este aspecto, ya que tienden a ser la principal fuente de fugas por estos métodos. Debemos concienciarles de que, cuanto menos rastro dejen en Internet, menos posibilidad habrá de que se filtre información relevante y sensible para la compañía.

Es conveniente informarles de que deben compartir en Internet (ya sea en redes sociales, archivos compartidos o conversaciones) información meramente esencial, fotos que no muestren nada que pueda resultar ser vulnerable y siempre sin la ubicación activa.

En general, esta formación es esencial. También es aconsejable tener un protocolo interno en el que se den las pautas sobre cómo subir archivos a Internet de forma correcta, para que todos los empleados dispongan de dicha información.

# PREGUNTAS FRECUENTES

## "AULA VIRTUAL" : CONSIDERACIÓN DE FORMACIÓN PRESENCIAL

Se considera **"aula virtual"** al entorno de aprendizaje donde el formador y alumnado interactúan, de forma concurrente y en tiempo real, a través de un sistema de comunicación telemático de carácter síncrono que permite llevar a cabo un proceso de intercambio de conocimientos a fin de posibilitar un aprendizaje de las personas que participan en el aula. Para que el "aula virtual" tenga validez pedagógica y se reconozca como formación permanente presencial debe reunir un conjunto de requisitos y, al mismo tiempo, debe asegurar que todos los actores, tanto alumnos como profesores, que quieran participar en el aula física ubicada en el centro de formación, tengan acceso inmediato, libre y en directo a dicha modalidad de formación presencial.

***Es un entorno donde el formador y el alumno interactúan de forma concurrente y en tiempo real.***

### REQUISITOS DE LOS SISTEMAS DE AULA VIRTUAL

1. Conectividad sincronizada entre la persona formadora y el alumnado participante. No será válido que los asistentes visualicen las sesiones en diferido.

2. La formación debe impartirse desde el aula física del centro de formación.

3. El número máximo de alumnos virtuales será de 25.

4. Bidireccionalidad en las comunicaciones. El alumnado participante debe de poder comunicarse con el profesor y con el resto del alumnado.

5. Registro de conexiones. El sistema de "aula virtual" que se utilice debe aportar un registro de las conexiones. Este registro sustituye a la hoja de control de asistencia.

6. El registro de conexiones del sistema de "aula virtual" debe de cumplir las siguientes condiciones:

   - Identificar visualmente a los participantes. El alumno no podrá desconectarse o ausentarse del curso, es decir, perderse su imagen desde el aula física del centro durante el desarrollo de la formación presencial.
   - Fechas en las que se han realizado las conexiones.
   - Indicar los tiempos de conexión de los alumnos.

1. A los efectos de actuaciones de seguimiento y control que procedan, contar con un mecanismo que posibilite la conexión del órgano inspector durante el tiempo de celebración del curso de formación. Se deberá proporcionar una dirección URL, usuario y contraseña que permita poder conectarse en cualquiera de las sesiones para que se hagan las comprobaciones que se consideren oportunas.

### COMUNICACIÓN DE LOS CURSOS DE FORMACIÓN PERMANENTE REALIZADOS A TRAVÉS DE "AULA VIRTUAL"

En las comunicaciones de los cursos de formación permanente que se vayan a impartir mediante "aula virtual" también se deberá incluir:

- Cronograma de las jornadas de formación.
- Acceso para la inspección con la dirección URL, usuario y contraseña, para poder acceder tanto a las sesiones de formación como a la revisión del registro de conexiones.

# INTERLOCUTOR POLICIAL SANITARIO: NOTICIAS

## JORNADAS DE FORMACIÓN DEPARTAMENTAL ORGANIZADAS POR EL HOSPITAL GENERAL DE VALENCIA SOBRE "VIOLENCIA DE GÉNERO DESDE LA PERSPECTIVA SANITARIA INTERNACIONAL" .

Esta jornada fue la última de las seis jornadas que se organizaron desde el Hospital General Universitario de Valencia, dentro de su plan de formación departamental, habiendo formado durante las mismas a más de 800 profesionales relacionados con el sector sanitario.

Estas jornadas, en las diferentes convocatorias de los meses de febrero, abril y junio, se han dirigido a personal de enfermería de atención primaria, a TCAE (técnicos en cuidados auxiliares de enfermería) y a auxiliares administrativos, junto a celadores de Atención Primaria, y han sido impartidas por la Interlocutora Policial Territorial Sanitaria de Valencia.

Dentro de esta ponencia, y como introducción a la misma, la Interlocutora Policial Sanitaria aprovechó la ocasión para dar a conocer dicha figura como persona de contacto entre el sector sanitario y la Policía Nacional, la aplicación AlertCops y la existencia de jornadas de formación para prevención de agresiones a sanitarios.


## FORMACIÓN A SANITARIOS DE CUENCA: PREVENCIÓN Y RESPUESTA ANTE AMENAZAS, INSULTOS Y AGRESIONES

La formación se celebró en el aula magna de la facultad de Bellas Artes de la capital conquense, y fue inaugurada por la Delegada de Gobierno en Cuenca acompañada del Jefe de la Comisaría Provincial y del Jefe de la UCSP e Interlocutor Policial Nacional Sanitario.

Ha sido organizada por la Policía Nacional a través de la Comisaría Provincial de Cuenca y la Unidad Central de Seguridad Privada (UCSP) de la Comisaría General de Seguridad Ciudadana.


## DÍA INTERNACIONAL DE LA MATRONA EN JAEN.

El **Día Internacional de La Matrona** se celebró en el Ilustre Colegio Oficial de Enfermería de Jaén. Al evento acudió en representación de la Policía Nacional el jefe de la Unidad Territorial de Seguridad Privada como Interlocutor Policial Territorial Sanitario.

# INTERLOCUTOR POLICIAL SANITARIO: NOTICIAS

## FORMACIÓN A SANITARIOS DE LEÓN

Fueron impartidas por el Interlocutor Policial Territorial Sanitario de León en el colegio oficial de enfermería. Esta formación contó con la asistencia de más de treinta enfermeras, y se trataron entre otros temas, técnicas básicas para prevenir las agresiones y legislación sobre la materia.

## FORMACIÓN A PERSONAL SANITARIO DE LA "MUTUA ASEPEYO" EN GUADALAJARA.

Durante la misma se instruyó al personal sanitario sobre una serie de pautas de actuación, con el objetivo de evitar posibles agresiones. Esta formación fue llevada a cabo en las instalaciones de "Mutua ASEPEYO" en Guadalajara, agradeciendo los asistentes la formación del Interlocutor Policial Territorial Sanitario.

## FORMACIÓN EN EL HOSPITAL SAN AGUSTÍN DE LINARES.

La Comisaría Local de Linares, con la colaboración del Interlocutor Policial Territorial Sanitario de la Provincia de Jaén, impartió en el Hospital San Agustín de Linares, una charla relacionada con las agresiones a los profesionales de la salud. El objetivo de la charla fue asesorar a los sanitarios en la adopción de medias para prevenir y reaccionar antes posibles agresiones, así como concienciar de la necesidad de interponer denuncia por tales hechos.

## CHARLA SOBRE MEDIDAS POLICIALES A ADOPTAR FRENTE A AGRESIONES A PROFESIONALES SANITARIOS EN MURCIA

La Unidad Territorial de Seguridad Privada e Interlocutor Policial Territorial Sanitario, impartió charla sobre medidas policiales a adoptar frente a agresiones a profesionales de la salud, la cual tuvo lugar en dependencias anexas al Hospital RIBERA MOLINA, en Molina de Segura, (Murcia), dirigida a profesionales del sector de la sanidad, asistiendo el Director del centro Sanitario, así como, el Director de Seguridad del Departamento de Seguridad del Grupo RIBERA SALUD, asistiendo un total de 50 personas.

## "TROFEOS DE LA SEGURIDAD TIC "

Nueva edición del Certamen Internacional **"TROFEOS DE LA SEGURIDAD TIC "**, instituidos por la revista Red Seguridad., a la que acudió el Comisario General de Seguridad Ciudadana, que participó en la entrega de trofeos.


## SECURITY FORUM 2023.

El sector de la seguridad celebró uno de los encuentros más importantes del año, el Security Forum, que contó con la presencia diversas unidades de Policía Nacional,.

En el espacio de Expert Panel se desarrollaron temas de actualidad, contando con las ponencias del Comisario Principal, jefe de la Unidad Central de Seguridad Privada, y de otros miembros de esta Unidad, pertenecientes a la Brigada Central de Inspección e Investigación.

## EL MINISTRO DEL INTERIOR PRESIDIÓ LA SEGUNDA REUNIÓN DE LA COMISIÓN NACIONAL DEL BICENTENARIO DE LA POLICÍA NACIONAL.

Esta segunda reunión sirvió para aprobar el programa de actos de esta celebración. El programa aprobado incluye diferentes tipos de actividades institucionales, culturales, lúdicas y divulgativas, que comenzarán a realizarse en el último trimestre de este 2023 y que alcanzarán su cenit a lo largo de todo el año 2024.

En su intervención, el Ministro destacó que se trata de una programación que *"marca la 'hoja de ruta' de una celebración histórica que queremos llevar a todo el territorio nacional y a todos los ámbitos de la sociedad"*, porque "*queremos hacer partícipes del Bicentenario a todos los ciudadanos*".

## ÚLTIMOS CAMBIOS EN JEFATURAS SUPERIORES DE POLICÍA.

Se ha procedido al nombramiento de los Jefes Superiores que a continuación se detallan:

- Comisario Principal D. **Florentino Martín Parra** en la JSP de **Aragón**
- Comisario Principal D. **Francisco López Gordo** en la JSP de **Ceuta.**

## LA UCSP DETIENE AL RESPONSABLE DE UN CENTRO DE FORMACIÓN POR FALSEDAD DOCUMENTAL

El Grupo Operativo de Investigación de la UCSP ha detenido recientemente al responsable de un centro de formación de seguridad privada por haber falsificado diferente documentación relacionada con el centro de formación, entre la que se encontraban resoluciones de adquisición en régimen de alquiler de armas y cartuchería. La investigación continua abierta en el ámbito administrativo en relación a supuestas infracciones a la normativa de seguridad privada.

# NOTICIAS

## JORNADAS FORMATIVAS A PERSONAL DE SEGURIDAD PRIVADA SOBRE ACTUACIONES OPERATIVAS EN ESTADIOS DE FÚTBOL EN GIJÓN.

Organizadas por la Policía Nacional y el **Departamento de Integridad y Seguridad de LaLiga de Fútbol** en las instalaciones del Estadio El Molinón-Enrique Castro "Quini" de Gijón (Asturias), se llevaron a cabo estas jornadas, como continuación a las que se vienen impartiendo en otras ciudades del país..

Fue inaugurada por el Comisario, Jefe de la Unidad de Coordinación Operativa de la Comisaría Local de Gijón, y las ponencias fueron impartidas por expertos de la Oficina Nacional de Deportes, de la UIP, de la Unidad Central de Seguridad Privada y de Participación Ciudadana de la Comisaría Local, así como por los integrantes del Departamento de Integridad y Seguridad LaLiga.

## CONTRATACIÓN DE LOS SERVICIOS DE SEGURIDAD PRIVADA DE APOYO A LA SEGURIDAD EXTERIOR EN CENTROS PENITENCIARIOS DE LA SEGURIDAD.

El Consejo de Ministros ha autorizado a la Secretaría de Estado de Seguridad la contratación de los servicios de seguridad privada de apoyo a la seguridad exterior en centros penitenciarios dependientes del Ministerio del Interior, contrato que estaría vigente durante los próximos dos años.

Desde el año 2014 y hasta la actualidad, los centros penitenciarios dependientes del Ministerio del Interior están custodiados por las fuerzas y cuerpos de seguridad del Estado, y además se cuenta con los servicios de apoyo de empresas de seguridad privada en tareas como son la vigilancia desde puestos fijos o el control de accesos y de los circuitos cerrados de televisión y control, con resultados muy positivos.

## NUEVO TÍTULO DE FORMACIÓN PROFESIONAL DE GRADO MEDIO DE TÉCNICO EN SEGURIDAD

El Consejo de Ministros, a propuesta del Ministerio de Educación y Formación Profesional (MEFP), ha aprobado la creación de este título, perteneciente a la familia profesional de Seguridad y Medio Ambiente.

Este curso tendrá una duración de 2000 horas, y esta iindicado para formar a los aspirantes en materia de vigilancia y protección de bienes y personas en espacios públicos y privados, tanto en entornos urbanos como naturales, en desarrollo de la normativa recogida en la normativa vigente. Está vinculado a ocupaciones como vigilantes de seguridad, escoltas o guardas rurales y sus especialidades, así como a otras asociadas a la seguridad pública.

## FORMACIÓN SOBRE ATAQUES A CAJEROS AUTOMÁTICOS PARA DEPARTAMENTOS DE SEGURIDAD DE LOS BANCOS

La UCSP organizó una formación dirigida a integrantes de departamentos de seguridad del sector bancario y financiero sobre ataques con explosivos a cajeros automáticos que impartieron especialistas de la Unidad Central de TEDAX-NRBQ de Policía Nacional en el complejo policial de Canillas.

La jornada fue clausurada por el Jefe de la Unidad Central de TEDAX-NRBQ.

# ACTOS DE CELEBRACIÓN DEL DÍA DE LA SEGURIDAD PRIVADA


**MURCIA**

**BADAJOZ**

**BURGOS**

# ACTOS DE CELEBRACIÓN DEL DÍA DE LA SEGURIDAD PRIVADA

VALLADOLID

LAS PALMAS DE GRAN CANARIA

OVIEDO

# ACTOS DE CELEBRACIÓN DEL DÍA DE LA SEGURIDAD PRIVADA

JAÉN

BARCELONA

SALAMANCA

# ACTOS DE CELEBRACIÓN DEL DÍA DE LA SEGURIDAD PRIVADA

CIUDAD REAL


A CORUÑA