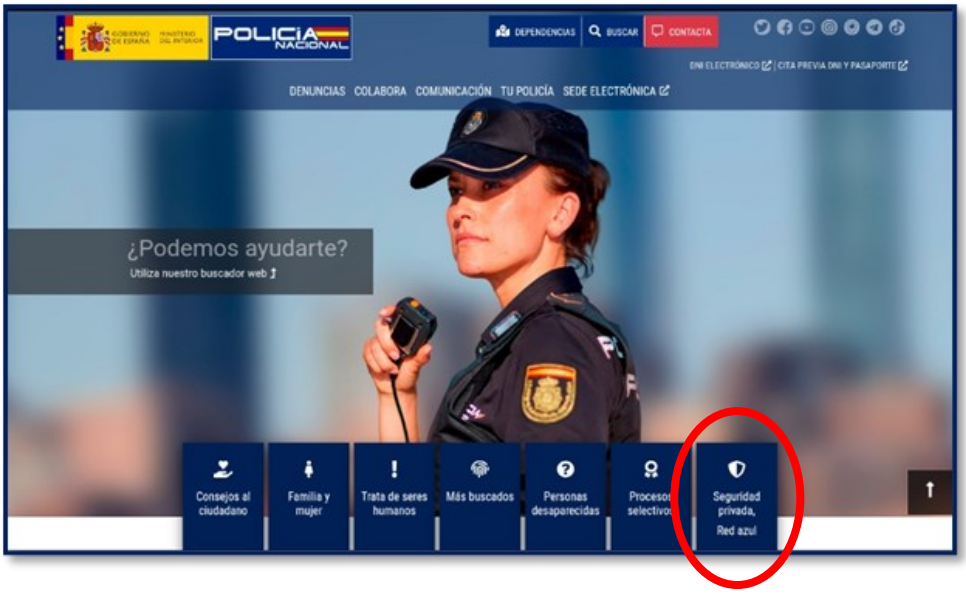
MARZO 2021 | Nº 16

BOLETÍN R@S

UNIDAD CENTRAL DE SEGURIDAD PRIVADA

LA NUEVA PÁGINA WEB DE LA POLICÍA NACIONAL DA UN TRATO PREFERENTE A LA SEGURIDAD PRIVADA

Estrenamos página web, afianzando nuestro compromiso con la transformación digital. La nueva interfaz cuenta con un diseño moderno que pretende optimizar la relación del ciudadano y facilitar el acceso a muchos trámites. Además, dispone de un acceso directo a la sección de seguridad privada, así como al área restringida de Red Azul.



WWW.POLICIA.ES

LA NUEVA PÁGINA WEB DE LA POLICÍA NACIONAL

La nueva web busca una relación más ágil y cercana con el ciudadano, continuando así su proceso de **transformación digital.** Esta imagen web destaca principalmente por su **modernidad y accesibilidad,** especialmente para personas mayores o con discapacidad, así como por **simplificar muchos de los trámites que los ciudadanos realizan electrónicamente ante la Policía.**

Además, esta nueva web **facilita el acceso al sector de la seguridad privada**. **Mediante un solo clic desde la página de inicio de la Policía Nacional se puede acceder** a la información sobre los procedimientos administrativos en relación a la seguridad privada, así como a los requisitos para la acreditación de los profesores de los centros de formación de seguridad privada. De igual forma, se accede directamente **a las áreas tanto de Red Azul, como del Programa Vigila.**

www.policia.es

"Allá donde esté la Seguridad Privada, está la Policía Nacional"

LA VENTANA DEL R@S
"LA SEGURIDAD PRIVADA Y LA PROTECCIÓN DE DATOS PERSONALES"

AUTOR: IGNACIO CARRASCO SAYALERO. ABOGADO ASIS ESPAÑA

El Reglamento Europeo 679/2016 de Privacidad y la Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales respecto a la privacidad (datos personales) ha supuesto un cambio de paradigma en los principios y derechos fundamentales de privacidad e intimidad.

Por su propia naturaleza, las actividades de seguridad son intrusivas respecto a los principios y derechos fundamentales de privacidad e intimidad. La observación sistemática, la investigación, el registro y comprobación de hechos de las actividades de las personas son actividades reservadas al Estado. Y la seguridad pública -y la privada- son las garantes de que dichas actividades se realizan cumpliendo la ley.

¿Las empresas de seguridad están obligadas a disponer de un Delegado de Protección de Datos, DPD?

El Reglamento Europeo de Protección de Datos 679/2016, en su artículo 37, establece los criterios para designar un DPD, y que se resumen en: si es AAPP o entidad pública; si la entidad trata datos de manera habitual o sistemática; o si los datos que trata son de gran volumen, sensibles o afectan a un sector de población significativo por cifra absoluta o por área geográfica.

Para evitar cualquier tipo de duda, el legislador español especificó en la Ley Orgánica 3/2018, artículo 34, una serie de sectores que, independientemente de si eran evaluables según los requisitos del artículo 37 del Reglamento, estarán obligados a tener DPD. Entre otros los distintos sectores y apartados: Enseñanza, Salud, Financiero, Seguros, *Utilities (energía, gas, telco)* y un largo etcétera,… y específicamente en su apartado ñ) Empresas de Seguridad.

¿Cómo se designa el DPD? ¿Quién puede ser DPD?

El DPD puede ser interno o externo. Si es externo –persona física o jurídica- deberá tener conocimientos profundos en derecho y acreditar suficiente practica en materia de Protección de Datos mediante certificación, según establece el artículo 35 de la LO 3/2018. También es recomendable –diría imprescindible- que conozca el derecho sectorial de la actividad de la empresa o entidad para la que trabaja y que tenga experiencia en el procedimiento administrativo común. En la práctica los DPD más cotizados son abogados en ejercicio con experiencia, tanto en privacidad como en la sociedad de la información, así como en el sector para el que trabajen.

En caso de designación interna, aunque los DPD puedan tener otras funciones, solamente podrán confiársele esta tarea si no tiene incompatibilidad. La AEPD emitió un informe en el que indica claramente que los directivos de una entidad que tengan competencias sobre datos personales NO puedan ejercer como Delegados de Protección de Datos de dicha entidad, por conflicto de intereses. Entre los cargos incompatibles están Administradores y Gerentes, Directores de RRHH, Directores Médicos, Directores de Marketing, Directores Comerciales y Financieros, y cargos similares… entre los que se incluye a los Directores de Seguridad.

¿Desde cuándo es obligatorio tener un DPD? ¿Es causa de sanción no disponer de un DPD estando obligado?

Desde el 25 de mayo de 2018 con la entrada en vigor del Reglamento UE 679/2016, para las entidades afectadas por su artículo 37. Y desde el 7 enero de 2019, expresamente, para las entidades y sectores designados en el artículo 34 de la LO 3/2018.

Esto es, desde hace más de DOS años que las Empresas de Seguridad deberían tener ya designado un DPD y haberlo comunicado a la AEPD, Agencia Española de Protección de Datos. Y aún hoy muchas empresas piensan que su "consultora" *low cost* ha cumplido con su deber…. ¡Incluso hay quien opina que no es obligatorio!

NO tener un DPD designado, cuando es entidad obligada, es causa de sanción grave. El artículo 73, dice en su apartado V:

v) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica."

"LA SEGURIDAD PRIVADA Y LA PROTECCIÓN DE DATOS PERSONALES"

AUTOR: IGNACIO CARRASCO SAYALERO. ABOGADO ASIS ESPAÑA

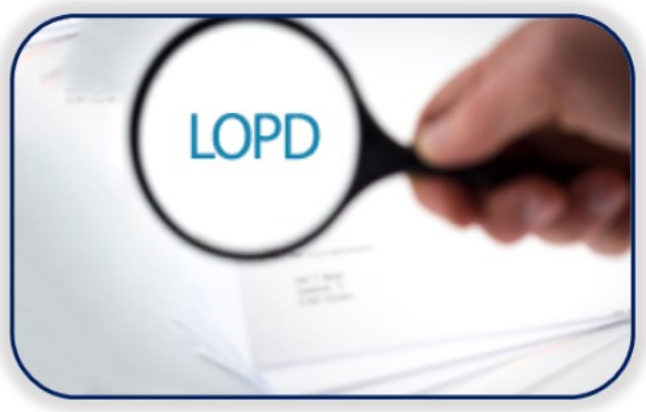
El art. 83.4 del RGPD establece que este tipo de infracciones se sancionarán, con multas administrativas de hasta 10.000.000 EUR o incluso hasta al 2 % del volumen de negocio anual global. ¡Para pensárselo!

Recientemente, en el Procedimiento Nº: PS/00251/2020, una empresa de seguridad española fue sancionada por no tener designado un DPD. A pesar de que se ponderaron varios atenuantes, le fue impuesta una multa por la AEDP de 50.000 EUR.

Las funciones del DPD también se describen en el Reglamento Europeo 679/2016 en su artículo 39. Básicamente es el responsable e interlocutor de la empresa ante la AEPD.

Su labor es de verificador y de *"pepito grillo"*. No es su misión realizar auditorías ni evaluaciones de impacto. Ni verificar los sistemas de gestión de información. Cuestión muy diferente es que un DPD cualificado pueda hacerlo. ¡Claro que puede! Y muy bien.

Un DPD calificado ayudará a analizar las necesidades reales y los puntos de riesgo más relevantes, recomendará plataformas adecuadas de gestión, detectara fallos en los flujos de información, y puntos débiles que puedan ser causas de brechas de seguridad, colaborará con el departamento de *compliance. Y* si es experto en normativa sectorial de seguridad privada, le ayudara en la armonización con las normativas de seguridad de información, confidencialidad y secretos empresariales, PIC, NIST e incluso ISO y UNE-EN.



LA PROTECCIÓN DEL TRANSPORTE DE METADONA POR EMPRESAS DE SEGURIDAD PRIVADA

La metadona es un opiáceo sintético que se administra sustituyendo a otros opiáceos de forma progresiva en el tratamiento de desintoxicaciones de personas drogodependendientes, con el fin de reducir gradualmente su adicción. Estas aplicaciones hacen que la metadona tenga en cierta medida un interés especial, que requiera de una mayor protección durante su distribución.

En este artículo se analizarán algunas cuestiones relacionadas con el servicio de protección que puede prestar la seguridad privada durante el transporte de esta sustancia.

¿Qué tipo de empresa de seguridad puede prestar el servicio de protección durante el transporte?

En primer lugar, se debe tener presente lo dispuesto en el art. 2 de la Ley 5/2014 de Seguridad Privada, donde se define actividad de seguridad privada como "*los ámbitos de actuación material en que los prestadores de servicios de seguridad privada llevan a cabo su acción empresarial y profesional".*

En su art.5 se describen estas actividades de seguridad privada, contemplándose, entre otras, las siguientes:

- *Art. 5.1. a) "La vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como las personas que pudieran encontrarse en los mismos".*
- *Art. 5.1. c) "El depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores, joyas, metales preciosos, antigüedades, obras de arte u otros objetos que, por su valor económico, histórico o cultural, y expectativas que generen, puedan requerir vigilancia y protección especial".*
- *Art. 5.1. e) "El transporte y distribución de los objetos a que se refieren los dos párrafos anteriores",* el cual hace referencia a los apartados c) y d) del mismo artículo.

En este sentido, la metadona podría estar incluida dentro de los objetos que, por su valor o expectativas que generen, se describen en el apartado c) del art. 5.1, contemplándose como actividad de seguridad privada tanto su depósito como su transporte y distribución, entre otras conductas.

Este servicio, ¿se debe prestar por vigilantes de seguridad con o sin armas?

Según el art. 40 de la ley referida anteriormente, se regulan los servicios de seguridad privada que se prestan con arma de fuego, entre los que se incluyen en el punto 1 apartado a) *"Los de vigilancia y protección del almacenamiento, recuento, clasificación y transporte de dinero, valores y objetos valiosos*".

Además, en el punto 2 de este mismo artículo, se hace referencia a que "*Reglamentariamente se determinarán aquellos supuestos en los que, valoradas circunstancias tales como localización, valor de los objetos a proteger,* (…) *podrá autorizarse la prestación de los servicios de seguridad privada portando armas de fuego".*

¿Cuál es el número de vigilantes que deberán realizar esta labor de protección?

La determinación del número de vigilantes de seguridad va a depender de si se utiliza un vehículo blindado o no.

A la vista del art. 33 del RD 2364/1994 por el que se aprueba el Reglamento de Seguridad Privada, se establece que en el caso de utilizarse vehículos blindados, obligatoriamente habrá de disponerse de tres vigilantes de seguridad armados. Atendiendo a factores tales como el valor de la mercancía, la modalidad de entrega o la periodicidad del transporte, el servicio podrá realizarse con otro tipo de vehículos de la propia empresa, efectuándose la protección por uno o dos vigilantes, según los casos, siempre dotados de arma de fuego. En el punto 6 del art. 21 de la Orden INT/314/2011, sobre empresas de seguridad privada, el cual se puede aplicar al supuesto concreto del transporte de metadona, se permite "*realizar estos transportes utilizando otro tipo de vehículos, propios o ajenos, contando con la protección de dos vigilantes de seguridad como mínimo, que se deberán dedicar exclusivamente a la función de protección e ir armados*".

Conclusiones

En caso de contratar un servicio de seguridad privada para la protección del transporte de la metadona, éste solo puede ser prestado por una empresa de seguridad autorizada para desarrollar la actividad de transporte referida en el art. 5.1.e) de la Ley de Seguridad Privada. Los servicios de las empresas autorizadas únicamente para desarrollar la actividad del artículo 5.1.a) de esa misma ley no pueden abarcar ninguna modalidad de transporte de mercancías, sean estas peligrosas, valiosas o de cualquier otra naturaleza.

El tipo de vehículo y el número de vigilantes pueden adaptarse a las concretas circunstancias, pero al tratarse de un transporte de seguridad, dicho servicio debe prestarse con la protección de armas de fuego.

¿Quién es el encargado de visualizar la imágenes cctv en una comunidad de propietarios?

Según el párrafo a) del apartado 1 artículo 5 de la Ley de Seguridad Privada, se considera entre las actividades de seguridad privada "*la vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos.*"

Además, el art. 6, donde se especifican las actividades compatibles de Seguridad Privada, se establece en su apartado 2 que:

"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: (…)*

d) Las 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. *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."***

Estas consideraciones se completan con el artículo 42, sobre los servicios de videovigilancia, que expone lo siguiente:

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

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

No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras ***cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada".***

Si se extravía la cartilla profesional, se debe solicitar un duplicado a la Unidad Territorial de Seguridad Privada correspondiente. Pero ¿Qué ocurre con todos los cursos sellados, menciones honoríficas, sanciones, etc. contenidos en ella?

En relación con los cursos contenidos en la cartilla extraviada, se entiende que el vigilante estará en posesión de los diplomas correspondientes, por lo que podrán volver a anotarse en la nueva.

Las sanciones no figuran en las cartillas profesionales.

Cuando se otorga una mención honorífica, en el acto se hace entrega de un diploma, con el que se podrá acreditar ese reconocimiento nuevamente.

Por último, de las altas y bajas de puestos de trabajo, queda siempre constancia en el Registro Nacional de Seguridad Privada.

Por ello, si se produce la pérdida o extravío de la cartilla profesional, cuando se acuda a solicitar el duplicado, es conveniente aportar toda esta documentación y anotar los datos de interés, así como una foto tamaño carné.

CIBER R@S: NORMATIVA
NUEVA ESTRATEGIA DE CIBERSEGURIDAD DE LA UE

FUENTE: EC.EUROPA.EU

Con el fin de proteger a todos los integrantes de la Unión Europea, la Comisión Europea ha elaborado una nueva Estrategia que abarca hasta 2025. Se centra en unas áreas prioritarias de actuación para ayudar a mejorar la seguridad de aquellos ciudadanos que viven en Europa.

Se pretende garantizar que la política de seguridad de la UE refleje el cambiante panorama de amenazas, creando una resiliencia sostenible a largo plazo, involucrando a las instituciones y agencias europeas, gobiernos, sector privado y reuniendo a las distintas políticas que afectan directamente a la seguridad.

LOS CUATRO PILARES DE LA ESTRATEGIA

Para garantizar la seguridad del entorno, la estrategia desarrolla una serie de medidas a tener en cuenta durante los próximos cinco años. Estas pautas de actuación europea se dirigen hacia cuatro prioridades estratégicas:

1.- Un entorno de seguridad que resista al paso del tiempo.

Para viajar, trabajar o disfrutar de servicios públicos esenciales, entre otras actividades que realizamos en nuestra vida cotidiana, existen numerosas infraestructuras claves, tanto en línea como fuera de línea. La UE ayuda a los Estados miembros a lograr una mayor protección física y unos sistemas de detección adecuados necesarios para garantizar estos servicios.

La sociedad y la economía actualmente son factores en vías de desarrollo digital, por lo que la ciberseguridad pasa a ser una cuestión de vital importancia en nuestra sociedad. Si una infraestructura crítica sufre incidencias a causa de un ciberataque, estas alteraciones pueden extenderse inmediatamente a las actividades de otras. Estas consecuencias, en última instancia afectan gravemente a los hogares, los servicios financieros y las empresas.

Además, debido a la pandemia de COVID-19, se ha incrementado el uso de las tecnologías y, a consecuencia de ello, también los ataques malintencionados, que intentaron beneficiarse del uso del teletrabajo, por ejemplo. Además, los servicios sanitarios esenciales se vieron perturbados en el momento de mayor presión, por lo que la UE debe adaptar sus capacidades al ritmo de la realidad.

2.- Hacer frente a las amenazas cambiantes.

La globalización, la libre circulación y la transformación digital siguen aportando prosperidad a nuestras vidas. Se trata de procesos en constante evolución y, derivado de ello, la seguridad igualmente debe de caracterizarse por tener un desarrollo dinámico que haga frente a las amenazas cambiantes y de diferente naturaleza. Ejemplos de estos ataques son: el aumento de los **programas maliciosos** y del robo de datos; la infiltración de **medicamentos falsos y adulterados** en la cadena de suministro legal de productos farmacéuticos o el crecimiento exponencial del **material pornográfico infantil online.**

El auge del internet y el recurso creciente a la inteligencia artificial aportarán, además de nuevos beneficios, una serie de riesgos.

Por otro lado, el auge de internet lleva aparejado de manera irremediable otros riesgos que se deben minimizar. Es necesario **adoptar medidas concretas** para hacer frente a las amenazas para los ciudadanos tales como el **terrorismo**, el **extremismo** o los **abusos sexuales de menores,** buscando un equilibrio entre seguridad y el respeto de nuestros derechos fundamentales. Una **prioridad clave** a este respecto es **prevenir y combatir** la propagación **de contenidos ilícitos online.**

3.- Proteger a los europeos frente al terrorismo y la delincuencia organizada.

El terrorismo sigue siendo hoy en día una amenaza importante para la UE. La delincuencia organizada sigue aumentando y opera cada vez más de manera internacional y transfronteriza. La UE debe proporcionar nuevos instrumentos para la aplicación efectiva de las leyes y llevar a cabo una lucha eficiente contra este tipo de criminalidad.

En este sentido, es necesario establecer medidas para apoyar a los Estados miembros en la lucha contra la radicalización. La aplicación de la **nueva Agenda de Lucha contra el Terrorismo de la UE** y las actividades de la **Red para la Sensibilización frente a la Radicalización** son dos instrumentos englobados dentro de este

objetivo, que también incluye el trabajo realizado por Europol y Eurojust a través de una estrecha cooperación con los Estados miembros.

4.- Un ecosistema de seguridad europeo sólido.

Para poder lograr una verdadera ´"unión de seguridad" se requiere que este aspecto sea un afán común a todos los Estados Miembros. Para ello, la UE puede ayudar a aunar los comunes esfuerzos de los cuerpos y fuerzas de seguridad, las autoridades judiciales, los gobiernos, los ciudadanos y el sector privado. La capacidad de la UE de innovar es también una herramienta estratégica para contrarrestar las amenazas actuales y anticiparse a los riesgos y oportunidades futuras.

Resulta crucial la existencia de **un intercambio de información eficaz,** así como una cooperación oportuna entre las autoridades policiales y judiciales entre los diferentes países en la lucha contra la delincuencia y el terrorismo. Indistintamente, contar con unas fronteras exteriores sólidas son también esenciales para proteger nuestra Unión frente a aquellos que pretenden hacernos daño.

Por último, es importante destacar que la sensibilización con respecto a las cuestiones de seguridad, junto con la adquisición de las capacidades necesarias para hacer frente a las potenciales amenazas, son dos aspectos fundamentales para construir una sociedad más resiliente y mejor preparada, tanto en el ámbito empresarial, como en el de la Administración y la ciudadanía.

INFORME COMPLETO

CIBER R@S: NORMATIVA
INFORME DE LA UNE DE APOYO A LA NORMALIZACIÓN A LA TRANSFORMACIÓN DIGITAL

FUENTE: UNE.ORG

A finales del pasado año 2020, la Asociación Española de Normalización (UNE) publicó el informe Apoyo de la Normalización a la Transformación Digital. Este documento tiene como objetivo ayudar a las empresas y a la Administración españolas a conseguir el éxito en el proceso de digitalización.

Con motivos de la actual crisis causada por el coronavirus, la transformación digital se ha visto acelerada en la gran mayoría de las empresas. Esto hace necesario la existencia de una armonización de normas y buenas prácticas para poder lograr una digitalización exitosa, junto con la opinión consensuada de expertos en diferentes áreas tales como la inteligencia artificial, la ciberseguridad, big data, etc.

Fruto de esta necesidad se han creado numerosos comités técnicos en las diferentes áreas posteriormente referenciadas que, además de unificar criterios, canalizan la opinión de los expertos españoles hacia los foros internacionales y de la Unión Europea encargados de la elaboración de normas relativas a la transformación digital y transición ecológica.

Las 16 áreas temáticas estratégicas de estandarización son:

1. Tecnologías habilitadoras digitales
2. Economía del dato
3. Desarrollo del talento digital
4. Telecomunicaciones
5. Ciberseguridad
6. Ciudades inteligentes
7. Digitalización industrial
8. Sector Público
9. Comercio electrónico
10. Conectividad del automóvil
11. Digitalización en la construcción
12. Salud digital
13. Accesibilidad TIC
14. Contenido audiovisual digital
15. Transición ecológica
16. Innovación

Estas áreas temáticas constituyen los pilares de la transformación digital, manteniendo un lenguaje común que aporta uniformidad y confianza en los productos y servicios, a través de marcos robustos y fiables.

En este sentido, las normas UNE dan respuesta eficaz a los grandes retos de las empresas sirviendo además como un sólido apoyo de las Administraciones en relación con las políticas públicas. Ejemplo de ello es, tal y como se menciona en el informe, la aplicación de estas normas en orden a la consecución de los objetivos de la Agenda España Digital 2025.

INFORME COMPLETO

CIBER R@S: CONSEJOS
SE RESPONSABLE, PROTÉGETE

Desde la Unidad Central de Ciberdelincuencia de la Policía Nacional se quiere sensibilizar al sector de la Seguridad Privada sobre la importancia de que las empresas estén informadas y actualizadas en materia de ciberseguridad.

Los ataques *ransomware* (cifrado de sistemas informáticos y posterior exigencia de rescate para su liberación) se han convertido en una de las ciberamenazas más pujantes a nivel mundial.

Estos ataques poseen un enorme potencial destructivo, al hacer inaccesible toda la información de un sistema, incluyendo las copias de seguridad que no estén desconectadas de la red, convirtiéndolo en un conjunto de componentes electrónicos totalmente inoperante.

Su capacidad dañina es aún mayor por ir normalmente acompañado por una exfiltración previa de datos sensibles, que permite la extorsión de la víctima bajo la amenaza de hacerlos públicos.

En sus orígenes, estos ataques afectaban frecuentemente a particulares. Con el tiempo, se han ido profesionalizando y, en la actualidad, se dirigen frecuentemente a empresas e incluso infraestructuras críticas.

El *ransomware* es, hoy, la principal amenaza contra los sistemas TIC, pero no la única. Otros ataques basados en la infección por software malicioso (*malware),* como los troyanos bancarios, las herramientas de acceso remoto (RAT), o los *phising* para el robo de credenciales, se siguen detectando con alarmante frecuencia.

Todos ellos comparten algunas características comunes, como el bajo nivel de denuncia por miedo al daño reputacional; su mayor actividad como consecuencia del aumento del uso de las TIC en entornos laborales a causa de la pandemia del COVID-19; o la existencia de verdaderas organizaciones criminales detrás de los ciberataques; pero, sobre todo, en todos ellos:

EL FACTOR HUMANO, PARTICULARMENTE EL CORREO ELECTRÓNICO, ES EL ESLABÓN MÁS DÉBIL DE LA CADENA DE CIBERSEGURIDAD.

El correo electrónico, combinado con la falta de compromiso con la seguridad informática, son factores decisivos para sufrir un ataque *ransomware* o de otro tipos de *malware.*

Más de un 60 % de los correos electrónicos a nivel mundial contienen software malicioso, y está implicado en el 90 % de los ciberataques (datos 2018).

El doble ataque de exfiltración de datos y *ransomware* se ha identificado como la ciberamenaza de carácter delictivo más relevante en la actualidad.

Así, la Unidad Central de Ciberdelincuencia proporciona los siguientes consejos al personal del sector:

- Promociona una cultura de la seguridad TIC en tu empresa y fomenta la **CONCIENCIACIÓN** y la **FORMACIÓN** en todos los usuarios.
- Mantén actualizadas tus copias de seguridad, **NO CONECTADAS** a la red.
- Sospecha de cualquier correo electrónico con **PATRONES FUERA DE LO COMÚN**, no coherentes con tu actividad, o mal redactados.
- Comprueba las extensiones de los archivos, **NO TE FÍES DE LOS ICONOS.**
- Si el remitente es conocido y sospechas, **CONTACTA** con él para comprobar la veracidad del correo.
- Ante cualquier sospecha, **NO ABRAS EL CORREO** y comunica con tu servicio de seguridad TIC.
- Si crees haber sido víctima de un ciberdelito:
  - **Denuncia** ante Policía Nacional, o ponlo en conocimiento de **tu enlace de RED AZUL.**
  - Aplica la **regla NTN (No Toques Nada)** y no borres ninguna información antes de hablar con la policía, puede ser de gran relevancia en la investigación.

CIBER R@S: CONSEJOS

RECOMENDACIONES EN EL USO DE DISPOSITIVOS DURANTE LOS DESPLAZAMIENTOS

FUENTE: CCN CERT

En el desplazamiento, fuera del entorno controlado propio de una organización, la exposición de los dispositivos electrónicos ante posibles ataques se incrementa, tanto por el valor de la información personal y laboral que contienen, como por sus características en sí mismas. Se trata de objetos de fácil sustracción, especialmente en lugares muy concurridos como son aeropuertos, hoteles o conferencias, entre otros. Además, la facilidad de conexión de estos dispositivos a redes de comunicación aumenta potencialmente el riesgo de sufrir ataques informáticos.

Según el momento del desplazamiento, es recomendable seguir las pautas básicas detalladas a continuación:

1. ANTES DEL DESPLAZAMIENTO.

a) Control de la información:

- Almacenar la información en un dispositivo no conectado a redes de comunicación.
- Mantener una copia de dicha información en las instalaciones propias.
- No utilizar dispositivos extraíbles (memorias USB, tarjetas SD…) ya que su pequeño tamaño facilita el extravío o sustracción. De considerarse necesario portarlos y contengan información sensible, deberán ir cifrados.
- Los sistemas operativos (en los ajustes de seguridad) permiten cifrar todo el almacenamiento exigiendo definir una contraseña de bloqueo de pantalla para el dispositivo.

b) Seguridad en los dispositivos: se han de revisar y configurar todos los dispositivos electrónicos que se vayan a utilizar durante el desplazamiento, intentando llevar lo imprescindible y minimizar la exposición a la amenaza.

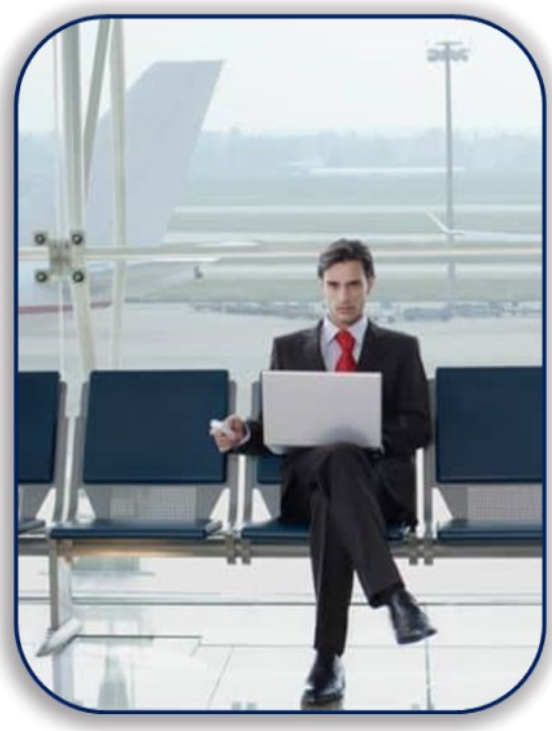
- Definir una contraseña de bloqueo de pantalla alfanumérica y compleja.
- No tener permisos de "administrador" del dispositivo.
- Mantener actualizada la última versión del sistema y *apps*, contar con un antivirus y un cortafuegos. Activar los mecanismos de protección BIOS/UEFI y gestores de arranque del dispositivo para ayudar a proteger el sistema contra ataques.
- Desinstalar aplicaciones no utilizadas, o inhabilitarlas en caso de que no se puedan desinstalar. Igualmente descargar las aplicaciones necesarias desde un origen fiable.
- Utilizar un servicio de VPN corporativa que no asocie la navegación al usuario o a un método de pago.

2. DURANTE EL DESPLAZAMIENTO.

a) Limitar el acceso a terceros: Además de definir una contraseña compleja, utilizar métodos de identificación biométrica.

b) Conexiones:

- Desactivar la conexión de datos (Wifi y 3/4G) siempre que no se esté utilizando, así como otras funcionalidades de conexión (USB, Bluetooth…). No realizar conexiones con dispositivos no confiables, ni redes Wifi abiertas.
- Algunos sistemas permiten utilizar una dirección física privada para reducir el seguimiento del dispositivo cuando se conecta a diferentes puntos Wifi.
- Dar preferencia a las alternativas de comunicaciones cableadas, en la medida de lo posible.



c) **Protección de datos:**

- Ante cualquier comportamiento anómalo, comunicarlo al responsable TIC del organismo.
- Para acceder a aplicaciones corporativas (correo electrónico, bases de datos…) utilizar una comunicación cifrada (VPN).
- En la medida de lo posible no utilizar el mismo dispositivo para navegar por Internet y para el tratamiento de información corporativa.

d) **Correo electrónico:** constituye uno de los vectores de infección más habituales. Además de la concienciación y el uso del sentido común, se recomienda:

- Ser especialmente cuidadoso con los correos recibidos. Comprobar que la dirección del remitente es conocida y confiable de no ser así no abrir el mensaje.
- No abrir ningún enlace ni descargar ningún fichero procedente de un correo electrónico con cualquier indicio considerado fuera de lo habitual.
- Evitar hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido, buscar primero información en motores de búsqueda.
- No habilitar la ejecución de macros en los documentos ofimáticos descargados, aunque el propio fichero lo solicite.
- Si fuera necesario enviar información sensible por correo electrónico, se debe cifrar el mensaje y/o adjuntos.

e) **Navegación web:**

- Asegurarse de que el navegador, así como *plugins* y extensiones, están actualizados a su última versión.
- Usar máquinas virtuales para navegar por Internet o habilitar la protección de aplicaciones, que favorecen el aislamiento del acceso a Internet y el consumo de la información corporativa.
- Revisar la privacidad del navegador: no aceptar cookies de terceros bloquear *pop-ups*, evitar sincronización de contraseñas evitar autocompletado de datos, etc.
- Utilizar un usuario sin permisos de administrador para navegar por Internet.
- Acceder únicamente a sitios web de confianza.
- Configurar el sistema operativo para forzar el uso de proveedores DNS seguros que incluya filtros de sitios maliciosos, contenido inapropiado o potencialmente dañino.

3. DESPUÉS DEL DESPLAZAMIENTO.

a) **Si existe la más mínima duda de haber sido víctima de un ciberataque no conectar los dispositivos electrónicos a la red corporativa.** Como mínimo es recomendable ejecutar un análisis antivirus. En casos más extremos puede ser necesario llevar a cabo un análisis forense o el reseteo a valores de fábrica del equipo.

b) **No es aconsejable conectar a la red corporativa los dispositivos extraíbles entregados por terceros sin revisión del responsable de seguridad TIC del organismo.**

c) **Informar con la mayor brevedad al departamento TIC de las incidencias detectadas.**

INFORME COMPLETO

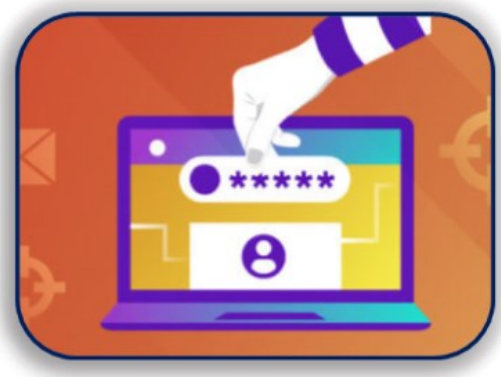
CIBER R@S: CONSEJOS
CIBERAMENAZAS CONTRA ENTORNOS EMPRESARIALES: UNA GUÍA DE APROXIMACIÓN AL EMPRESARIO

FUENTE: INCIBE

Para ayudar a las empresas a mantener unos adecuados niveles de ciberseguridad, evitando las principales amenazas, INCIBE, a través de **Protege tu empresa**, ha publicado '***Ciberamenazas contra entornos empresariales: una guía de aproximación para el empresario***'.

Desde las grandes corporaciones hasta las pequeñas pyme, todas las empresas gestionan información de gran interés, no solo para el funcionamiento de la propia empresa si no también para los ciberdelincuentes. Desgraciadamente, el objetivo de estos criminales no se limita únicamente a esta información, si no que los sistemas que la gestionan también son de su interés. A través de esos medios, pueden perpetrar nuevos fraudes o simplemente extorsionar a la empresa propietaria.

Estas amenazas de índole cibernética hacen que sea fundamental conocer sus principales métodos de actuación y saber identificarlas, para poder evitar sus efectos dañinos y reducir las vulnerabilidades de los sistemas de la empresa. La guía publicada por el INCIBE muestra de forma clara y sencilla las principales ciberamenazas, la vía para reconocerlas y cómo actuar en caso de ser víctima de una de ellas.



Principales ciberamenazas

La gran mayoría de los ataques que afectan a las empresas tienen en común dos factores: el correo electrónico y las comunicaciones. Por ello, es muy importante aprender a determinar si una notificación es de tipo fraudulenta o si realmente se trata de información fiable.

Numerosas pymes y autónomos utilizan habitualmente el correo electrónico como herramienta de trabajo, lo que le convierte en la vía preferida por los ciberdelincuentes para propagar sus campañas maliciosas. Esta frecuencia en su uso es lo que vuelve a esta herramienta peligrosa, ya que en muchas ocasiones las tareas se realizan de forma mecánica sin prestar demasiada atención, lo cual es conocido por los delincuentes. De esta manera, aprovechan para provocar infecciones por malware o accesos a páginas web fraudulentas.

Además, a través del correo electrónico consiguen atacar al eslabón más importante en la cadena de la seguridad, los empleados. Esto se debe a que los ataques basados en ingeniería social requieren mucho menos esfuerzo que otros tipos de ataques, y por lo tanto el beneficio es mayor. Algunas de las técnicas englobadas en este tipo de ciberataques son:

- **Impersonalización:** consiste en falsear la dirección del remitente. En los correos electrónicos es posible falsificar la dirección del remitente, mediante una técnica a la que se denomina *email spoofing*.
- ***Cybersquatting:*** se basa en modificar ligeramente el nombre de dominio, de forma que sea fácilmente reconocido como uno verdadero.
- **Falsear enlaces** que simulan enlazar a un sitio web legítimo cuando en realidad no es así.
- **Adjuntar documentos maliciosos**. Al hacer clic sobre ellos, se abre o descarga un archivo capaz de dañar el equipo.

Tener en cuenta estas ideas básicas sobre ciberataques resulta vital para que la continuidad del negocio no se vea afectada.

Decálogo de recomendaciones

Este decálogo supone una enumeración de recomendaciones a tener en cuenta por los empresarios para minimizar el riesgo de sufrir una incidencia de seguridad.

1. **Extremar** aún más las **precauciones** al recibir un correo electrónico procedente de un **remitente desconocido,** ya que puede tratarse de una maniobra maliciosa.
2. Tal y como se ha expuesto anteriormente, es necesario saber **reconocer si el remitente** del correo electrónico **está falseado** para evitar ser víctima de un ciberataque.
3. **Una alteración tan insignificante** como puede ser un solo carácter en el nombre de la página web o del correo electrónico puede llegar a **provocar un incidente de seguridad.**
4. **Ante intentos de redireccionarnos** a enlaces externos o documentos desde un mensaje de correo electrónico se han de **extremar las precauciones.** Es recomendable analizarlos con herramientas en línea o con el antivirus del dispositivo.

CIBER R@S: CONSEJOS
CIBERAMENAZAS CONTRA ENTORNOS EMPRESARIALES: UNA GUÍA DE APROXIMACIÓN AL EMPRESARIO

FUENTE: INCIBE

5. Mantener la **última versión disponible** de todos los dispositivos de la corporación, así como de las aplicaciones y herramientas que estos tienen instaladas.
6. Contar con **aplicaciones antivirus** instaladas y actualizadas.
7. **Poner en conocimiento de las** Fuerzas y Cuerpos de Seguridad del Estado (**FCSE**) y el centro de respuesta a incidentes de **INCIBE** cualquier incidente de seguridad.
8. Si el incidente **afecta a datos de carácter personal,** avisar también a la Agencia Española de Protección de Datos (**AEPD**).
9. El correo electrónico no es la única vía utilizada por los ciberdelincuentes. Prestar **atención también a llamadas telefónicas, SMS, redes sociales, chats...**
10. Cualquier solicitud que requiera **modificar datos bancarios** ha de ser **minuciosamente verificada** por un canal alternativo y confiable.
11. Los **correos de extorsión** mediante un supuesto vídeo privado son un fraude. **Eliminarlos directamente,** el vídeo no existe.
12. Utilizar **contraseñas robustas**, evitar repetir contraseñas en más de un servicio y, siempre que sea posible, habilitar un doble factor de autenticación.
13. Realizar **copias de seguridad de la información** de la empresa, actualizarlas periódicamente y comprobar que es posible su restauración.

INFORME COMPLETO

LA COLABORACIÓN ENTRE SEGURIDAD PRIVADA Y POLICÍA NACIONAL EN PALMA CONCLUYE CON DOS DETENCIONES Y LA INTERVENCIÓN DE TRES PISTOLAS Y UN DRON

La investigación comenzó cuando un vigilante de seguridad dedicado a la vigilancia y protección de una nave industrial del polígono de Son Noguera de Palma (Mallorca) localizó en la misma un armario que contenía diversas armas de fuego. Ante tal descubrimiento, alertó a la Unidad de Seguridad Privada de Palma, quien gestionó la información, haciéndose responsable de la investigación el Grupo II de Estupefacientes.

Días más tarde, los vigilantes de seguridad volvieron a alertar sobre la interceptación de un dron que accedió a esta misma nave.

Fruto de esta colaboración con la empresa de seguridad, se incautaron tres pistolas de fuego real con su correspondiente munición y un dron. Además, se detuvo a dos personas por un delito de coacciones.

LA POLICÍA NACIONAL ALERTA SOBRE UN INCREMENTO DE ESTAFAS A LAS ADMINISTRACIONES PÚBLICAS.

En las últimas semanas se está produciendo un incremento de estafas a las Administraciones Públicas, tales como intentos de fraudes al CEO (Chief Executive Officer) y fraudes BEC (Business Email Compromise). En ambos casos los delincuentes tienen que disponer de información sobre la víctima y su entorno para generar en la víctima la creencia de que está tratando con la persona suplantada.

En el caso de las Administraciones Públicas, las organizaciones criminales defraudadoras pueden obtener, vía online y sin rastro alguno, información pormenorizada sobre contratos establecidos por la Administración Pública y los altos cargos públicos responsables de su tramitación.

Los ciberdelincuentes desarrollan un engaño a través de correos electrónicos basado en datos precisos y pormenorizados de contrataciones reales, enfocándose en las empresas proveedoras como víctimas, tanto en la modalidad de pagos fraudulentos a un organismo público suplantado, como pagos fraudulentos entre contratista y subcontratista.

Para evitar que estos fraudes lleguen a cometerse, resulta necesario que tanto los responsables públicos de los departamentos de contratación, como las **empresas adjudicatarias y subcontratadas de contratos públicos extremen sus precauciones.** La detección de cualquier tentativa de estos tipos de fraudes debe ser puesta en conocimiento de la Policía Nacional a la mayor brevedad posible.

RECONOCIMIENTO A LA SEGURIDAD PRIVADA POR SU TRABAJO DURANTE LA PANDEMIA

El pasado 5 de febrero tuvo lugar en la Comisaría Provincial de Huesca una entrega de menciones honoríficas reconociendo la labor que desempeña el sector de la seguridad privada. Este acto debería de haberse realizado el pasado 21 de mayo, día de la seguridad privada, pero, con motivo de la crisis sanitaria del Covid-19, se vio obligado a aplazarse.

La Subdelegada del Gobierno, junto con el Comisario Provincial y el jefe de la Unidad Territorial de Seguridad Privada, hizo entrega de **8 menciones a personal del sector, reconociendo su labor especialmente durante el pasado año, donde los vigilantes de seguridad privada estuvieron en primera línea sumándose así en la lucha contra la pandemia. Igualmente se reconocía el esfuerzo de los directores y jefes de seguridad** que no sólo se han encargado de marcar las directrices y gestión de los recursos, sino que también han garantizado la continuidad del servicio.

LA POLICÍA NACIONAL Y EL SERVICIO SECRETO DE LOS EEUU DESARTICULAN UNA ORGANIZACIÓN QUE HABRÍA DEFRAUDADO MÁS DE 12 MILLONES DE EUROS

La Policía Nacional y el Servicio Secreto de EEUU llevaron a cabo la mayor investigación de ámbito internacional realizada hasta la fecha contra el fraude cometido con tarjetas bancarias. El macrooperativo permitió la **detención de 105 personas en España, Austria, Reino Unido y Grecia**, como presuntos autores de delitos de organización criminal, estafa, blanqueo de capitales, falsedad documental y tenencia ilícita de armas. Se han practicado 88 registros domiciliarios simultáneos en cuatro de estos países. La red desmantelada se dedicaba desde 2017 a la creación de empresas fantasma en Estados Unidos para, tras dotarlas de una falsa solvencia económica, solicitar la expedición de tarjetas de débito con el máximo importe disponible, bajo el pretexto de utilizarlas en sus viajes a Europa. Una vez en España, las tarjetas eran utilizadas en establecimientos conniventes (los cuales se llevaban una comisión del 15%) por elevados importes, aprovechando la diferencia de aceptación del pago existente entre los bancos americanos y españoles.

Mediante este procedimiento lograban realizar importantes compras y posteriormente vaciar las cuentas de efectivo, antes de que las entidades bancarias pudieran anular las operaciones. **Esta organización criminal, que tenía su base de operaciones asentada en un hotel de Miajadas (Cáceres), habría defraudado más de 12 millones de euros.**

La investigación, también ha contado con la participación de EUROPOL, así como de los cuerpos policiales de Grecia, Austria, Dinamarca, Reino Unido, Alemania, Polonia y Ucrania.

Como consecuencia del operativo se han bloqueado 87 cuentas con saldos que **superan el millón de euros;** se han intervenido 427.000 euros, 8.000 dólares y 600 coronas checas en efectivo; más de 200 tarjetas bancarias y 100 datáfonos; documentación falsificada; 14 vehículos de alta gama; 10 armas de fuego y varios machetes y cuchillos.

SEMINARIO SOBRE SEGURIDAD PRIVADA A LOS FUTUROS MANDOS DE LA POLICÍA NACIONAL

Durante los días del 8 al 11 de febrero de 2021 tuvo lugar en la Escuela Nacional de Policía el **Seminario "La estrategia de la Policía Nacional con la Seguridad Privada"**, dirigida a Inspectores de segundo curso de Escala Ejecutiva. El seminario fue organizado por el departamento de Ciencias Jurídicas de la Escuela, junto con el asesoramiento de la Unidad Central de Seguridad Privada.

Las diferentes ponencias fueron impartidas por el Comisario Principal de la UCSP, Manuel Yanguas Menéndez; el Comisario de la Brigada Central de Inspección e Investigación e Interlocutor Policial Sanitario, Javier Galván Ruiz; así como por el Jefe de la Sección de Colaboración, el Inspector Jefe David Bravo Núñez. Varios integrantes de la Unidad Territorial de Seguridad Privada de Ávila también participaron en estas jornadas.

Durante los tres días que duró el seminario se trataron diferentes temas de interés, tales como la Policía Nacional como Autoridad Nacional de Control del Sector, la colaboración entre seguridad pública y privada, así como los prestadores de servicios y el personal integrante del sector.

EL INTERLOCUTOR POLICIAL NACIONAL SANITARIO PRESENTA EL BALANCE DE ACTIVIDAD DEL AÑO 2020

El día 2 de marzo, tuvo lugar el acto de presentación de los datos que recogen la actividad de los interlocutores policiales nacionales sanitarios durante el pasado año. En la presentación participaron el Comisario General de Seguridad Ciudadana, el Jefe de la Unidad Central de Seguridad Privada y el Interlocutor Policial Nacional Sanitario, junto con representantes de los Colegios Nacionales Profesionales de Médicos, Enfermería, Odontología y Farmacia.

El trabajo de los interlocutores ha conseguido **reducir en un 33% las agresiones a profesionales de la salud en el año más dramático para este sector.** Desde su puesta en marcha en 2017, se mantiene una **tendencia descendente de los delitos sufridos por este colectivo,** lo cual ensalza la labor de los 59 agentes que constituyen los interlocutores policiales nacionales sanitarios, que, además de atender las agresiones, **han realizado hasta 8.000 contactos con el sector durante el estado de alarma, desde marzo hasta junio de 2020.**

Con el fin de seguir avanzando, se prevé la puesta en funcionamiento de actividades en el ámbito universitario, un curso a nivel nacional para los sanitarios en colaboración con la Organización Médica Colegial y campañas de sensibilización, junto al nuevo proyecto "**IPNS 21**", que tiene como objetivo el asesoramiento a profesionales de la salud en su propio puesto de trabajo, entre otras competencias.

RED AZUL 21: ÁVILA

El miércoles 3 de marzo, agentes de la Policía Nacional de la Comisaría General de Seguridad Ciudadana (Madrid) y de la Comisaría Provincial de Ávila se desplazaron a diferentes puntos de la capital abulense donde prestan servicio vigilantes de seguridad con el fin de reforzar la colaboración público-privada en seguridad. Este desplazamiento, enmarcado dentro del proyecto **RED AZUL 21**, afianza la relación de la Policía Nacional con los profesionales de la seguridad privada, tiene como objetivos conocer de primera mano sus inquietudes, prestarles asesoramiento y aclarar sus posibles dudas sobre la normativa de seguridad. Asimismo, se da a conocer el programa Vigila, el cual permite el acceso a todos los vigilantes de seguridad al área restringida de Seguridad Privada - RED AZUL de la página oficial de la Policía Nacional, www.policia.es. Para entrar en Vigila, los vigilantes de seguridad deben introducir su número de DNI, con la letra en mayúsculas, y su número de TIP (Tarjeta de Identidad Profesional).

AMPLIACIÓN DEL HORARIO DE LAS JORNADAS DE FORMACIÓN ONLINE EN MATERIA DE PREVENCIÓN ANTITERRORISTA PARA VIGILANTES DE SEGURIDAD

Con el fin de facilitar el acceso a nuestras jornadas formativas, **se ha ampliado el horario en el que se imparten, pudiendo realizarse por la mañana, por la tarde e, incluso, durante los fines de semana.**

Los vigilantes de seguridad, escoltas o guardas rurales interesados en recibir esta formación, la cual es computable cómo formación anual permanente, **pueden inscribirse remitiendo un correo electrónico a redazul@policia.es con su nombre y datos personales,** pudiendo indicar sus preferencias sobre el turno para realizar la formación.