GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

GUARDIA CIVIL
DIRECCIÓN GENERAL

BOLETÍN COOPERA

GUARDIA CIVIL - SEGURIDAD PRIVADA

Número 04/2023

ÍNDICE

1. TERRORISMO

COMUNICADO:

Participamos que las referencias, bajo este epígrafe contenido en Boletines anteriores, debido a razones de confidencialidad han dejado de ser publicadas. No obstante, los profesionales u otras organizaciones del sector de la seguridad privada adheridas al Programa Coopera que lo deseen, pueden seguir accediendo a esa información, previa solicitud a este SEPROSE.

2. ACTUALIZACIÓN NORMATIVA

2.1 LA DIRECTIVA NIS2 Y EL RESPONSABLE DE CIBERSEGURIDAD

Revista de Seguridad "Quorum" – Número 21 – FEBRERO/MARZO 2023
RAFAEL PEDRERA MACÍAS

El 27 de diciembre se publicaba en el Diario Oficial de la Unión Europea la Directiva UE 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, conocida coloquialmente como NIS2 (Network and Information Systems 2) por ser la actualización de la directiva NIS 2016/1148 que ya en su día supuso un revulsivo para las anticuadas formas de organizar la ciberseguridad nacional.

Vamos primeramente a echar un vistazo a la situación que había hasta su aparición.

El problema de la ciberseguridad, omnipresente hoy en día, en un pasado no tan lejano fue abordado en nuestro país por las distintas organizaciones que tenían algún tipo de responsabilidad en esta materia, pero de forma descoordinada. Por una parte, se recurrió a un convenio entre el INCIBE (Instituto Nacional de Ciberseguridad) el cual se ocupaba de los ciudadanos y PYMES, con el CNPIC (Centro Nacional de Protección de Infraestructuras Críticas), ampliando así su público objetivo; y por otro lado el CCN (Centro Criptológico Nacional) del CNI también abordó esta materia desde la perspectiva de los sistemas de información de la Administración y considerando también aquellas entidades de interés estratégico para la seguridad nacional. Esto, como es natural, llevó a un solapamiento de áreas de actuación con sus fricciones correspondientes entre las distintas organizaciones.

La trasposición de la Directiva NIS de 2016 en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información vino a deshacer entuertos en los distintos ámbitos de la ciberseguridad, estableciendo los siguientes principios:

- Protección de los servicios esenciales dependientes de las redes y sistemas de información, siendo estos servicios esenciales definidos en dos categorías: sectores estratégicos marcados por la Ley de Protección de Infraestructuras Críticas, por una parte, y por otra los proveedores de servicios digitales (DSP), esto es, entidades que, sin ser PYME, prestan un servicio digital; mercados online, motores de búsqueda o computación en nube.

- Notificación de ciberincidentes por parte de los responsables de los sistemas de información a las autoridades competentes. Las autoridades competentes varían según la naturaleza de la entidad afectada: para los operadores de infraestructuras críticas será la Secretaría de Estado de Seguridad del Ministerio del Interior a través del CNPIC, para los operadores de carácter público será el CNI del Ministerio de Defensa, a través del CCN. Para el resto de operadores, la autoridad sectorial correspondiente en cada ministerio.

- Se establecen asimismo los equipos de respuesta a ciberincidentes (también llamados CERT o CSIRT) correspondientes según la naturaleza del operador afectado. En España estos son el INCIBE-CERT para el ámbito privado y el CCN-CERT para el ámbito público. En el ámbito de la defensa, actuará el ES-PDEF-CERT, Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa.

- El Real Decreto-Ley 12/2018 es desarrollado por el Real Decreto 43/2021. De nuestro interés es el artículo 7 *"Responsable de la Seguridad de la Información"*, donde entre otras cosas se especifica en el apartado 1 que todo operador de servicios esenciales designará *"una persona, unidad u órgano colegiado, responsable de la seguridad de la información que ejercerá las funciones de punto de contacto y coordinación técnica con la autoridad competente y CSIRT de referencia".*

Una vez puestos en situación, nos vamos a centrar en este último aspecto. Nos metemos en la piel de este Responsable de la Seguridad de la Información (o ciber-seguridad) y nos preguntamos: ya sea nuestra entidad una infraestructura crítica o un proveedor de servicios digitales, ambos sometidos ya a una abultada serie de obligaciones**, ¿en qué nos vamos a ver afectados a partir de ahora?**

La Directiva NIS2. Nuevos sectores afectados

La NIS2 reemplaza a la NIS original para dotar de nuevas y más robustas medidas de ciberseguridad en sectores que define como "muy críticos" tanto del ámbito público como del privado, que son muy parecidos a los definidos en la también nueva Directiva 2022/2557. Esta última, conocida como Directiva de Ciberresiliencia, ha sido aprobada en paralelo con la NIS2, deroga la Directiva 2008/114/CE, que abordaba la protección de infraestructuras críticas europeas, y defines nuevos sectores y subsectores estratégicos en los que se localizan estas infraestructuras críticas, como por ejemplo el del Hidrógeno, tan de moda últimamente.

Los nuevos sectores muy críticos (subsector hidrógeno, servicios postales y de mensajería y gestión de residuos, etc.) se une a la ampliación del rango de lo que considera proveedores de servicios digitales, añadiendo proveedores de dominio de primer nivel, de servicios de centro de datos, de redes públicas de comunicaciones electronica y de servicios de confianza, entre otros.

Como hemos visto, se multiplica el número de Responsables de Ciberseguridad afectados por la norma. ¿Qué debemos, como tales, hacer ahora? Teniendo en cuenta que la NIS2 debe trasponerse antes de octubre del 2024, conviene ir preparando el terreno. El objetivo de esta directiva es eliminar las diferencias en los requisitos de ciberseguridad y de aplicación de las medidas entre los Estados de la Unión Europea, desglosando en capítulos el mecanismo

que tiene pensado para ello. Vamos a analizar cuáles de estos nos afectarían como Responsables de la Ciberseguridad.

Disposiciones Generales

En este capítulo es digno de reseñar qué define el tamaño de las empresas afectadas, que son aquellas que según la Recomendación 2003/361/CE sean medianas empresas o superen este tamaño en los sectores mencionados anteriormente. Independientemente, también lo serán las entidades de la administración central o regional cuya perturbación suponga un impacto significativo en las actividades sociales o económicas. También a aquellas que se encuentren definidas como entidades críticas con arreglo a la Directiva 2022/2557 ya mencionada. Estas entidades, esto es, medianas empresas y superiores de los sectores señalados, así como las entidades críticas, serán entidades esenciales. Por otra parte, aquellas entidades que presten servicios en estos sectores, pero no lleguen a esta categoría, serán clasificadas como entidades importantes.

La NIS2 no se aplicará a las entidades de la Administración pública que lleven a cabo sus actividades en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la garantía del cumplimiento de la ley.

Marcos de Ciberseguridad coordinados

En cuanto a la coordinación nacional, en España estamos muy avanzados ya que hicimos las tareas con la transposición de la NIS1. La Estrategia Nacional de Ciberseguridad, la designación de autoridades competentes, los puntos de contacto únicos y los CSIRT de referencia ya son una realidad para el Responsable de la Ciberseguridad. Como novedad tenemos la creación de una base de datos europea de vulnerabilidades, y para promover la comunicación de vulnerabilidades "los Estados miembros velarán por que las personas físicas o jurídicas que así lo soliciten puedan notificar de forma anónima una vulnerabilidad al CSIRT coordinador (a efectos de la divulgación coordinarla de las vulnerabilidades)". Esto supone una herramienta doble para el Responsable de la Ciberseguridad, por un lado, le

facilita la comunicación de vulnerabilidades descubiertas, sin poner en juego la "imagen" de su entidad, y por otra tiene acceso a un repositorio de vulnerabilidades que pueden afectar a sus sistemas, así como los parches asociados, alimentado por infinidad de entidades a nivel europeo.

Medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación.

Aquí nos encontramos con uno de los puntos centrales, la obligatoriedad de notificar. El pasado diciembre el Banco Central Europeo (BCE) multó a una Entidad con 3.145.000€ por no notificar en el plazo estipulado el haber sido afectada por un ciberataque. Las entidades supervisadas por el BCE tienen un plazo de dos horas desde su detección para comunicar cualquier ciberincidente significativo. Como podemos leer en el comunicado del BDE *"En febrero de 2019, fue objeto de un ciberataque cuando sus sistemas tecnológicos se vieron infectados por software malicioso. Respondió suspendiendo temporalmente los servicios de banca por internet y móvil, los servicios de cajeros automáticos y los servicios de pago SWIFT... la entidad remitió el informe requerido sobre el incidente 46 horas después del plazo estipulado"*. Ésta es la línea que se va a seguir con todos los operadores afectados por la NIS2, así que es conveniente tener los sistemas y protocolos de reporte de incidentes perfectamente establecidos. La notificación deberá realizarse al CSIRT o autoridad correspondiente, teniendo un plazo de 24 horas para la primera alerta temprana.

Por otro lado, la Directiva nos dice que el Estado velará por que se implementen medidas técnicas, operativas y de organización adecuadas. Entre ellas se encuentra la gestión de crisis, y hemos de esperar que fondos europeos respalden esta obligatoriedad.

La Directiva incide en este capítulo en facilitar a las entidades afectadas el intercambio de información sobre ciberamenazas, cuasi incidentes, vulnerabilidades, técnicas y procedimientos, indicadores de compromiso, etc., contando para ello con los medios técnicos necesarios, lo que se traducirá en un futuro el tener acceso a sistemas o plataformas con este tipo de información, con capacidad para volcar también nuestros análisis y poder mejorar nuestra ciberseguridad contando con lo aportado por la comunidad de Responsables designados por la NIS2. Plataformas de este tipo ya existen, pero es de sobra conocido el efecto de que cuanto más abiertas a más participantes son, la información que se llega a intercambiar disminuye en su calidad, puesto que los datos de vulnerabilidades y ciberincidentes, igual que sirven para mejorar sistemas, también sirven para atacarlos, y ante la duda de quién puede estar al otro lado, muchos optan por el silencio en lo tocante a qué está pasando en sus sistemas. El tener una plataforma de acceso restringido es una garantía de calidad de los datos.

Conclusiones

La actualización a la Directiva NIS2 amplía su objetivo y vuelve a incidir en los escalones directivos de la organización, exigiéndoles responsabilidades a la par que exhorta a las autoridades competentes de cada Estado para que supervisen el cumplimiento de la misma, con su correspondiente régimen sancionador. El Responsable de la Ciberseguridad pasa a las primeras filas de la organización con lo que ello conlleva, pero también cuenta con más respaldo legal y técnico a la hora de ejercer su función.

Asociación Profesional de la Guardia Civil. Unión de Oficiales (UO)
revista@unionoficiales.org

2.2 PUESTA EN MARCHA DEL PLAN OPERATIVO "OCIO SEGURO"

En noviembre de 2022, el Secretario de Estado de Seguridad estableció el reforzamiento de especial intensidad de las medidas incluidas en diferentes planes operativos y preventivos de la Secretaría de Estado de Seguridad, concretamente los siguientes:

- Plan de actuación y coordinación policial frente a los grupos violentos de carácter juvenil.
- Plan estratégico de respuesta policial al consumo y tráfico minorista de drogas en zonas, lugares y locales de ocio.
- Plan Director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos.
- Protocolo de actuación de las Fuerzas y Cuerpos de Seguridad del Estado respecto al control de las armas blancas y otros instrumentos peligrosos para la seguridad ciudadana.

Además de todo lo anterior, el fenómeno de "las violencias sexuales vulneran el derecho fundamental a la libertad, a la integridad física y moral, a la igualdad y a la dignidad de la persona" y se puede dar tanto en lugares públicos como privados, por tal motivo se debe prestar atención a la prevención sobre este fenómeno, la atención, el seguimiento y la protección de las víctimas de cualquier tipología de violencia sexual.

A tenor de lo anterior y al objeto de mantener e impulsar la actividad policial para erradicar las conductas referidas y teniendo en cuenta los resultados obtenidos en los últimos años, la Secretaria de Estado de Seguridad pone en marcha un nuevo **"Plan Operativo de respuesta policial al tráfico minorista y consumo de drogas en zonas, lugares y locales de ocio para el año 2023".**

Por tanto, este Plan persigue una doble finalidad, de un lado cumplir lo establecido en la Instrucción 3/2011, de la Secretaría de Estado de Seguridad "Plan Estratégico de respuesta policial al consumo y tráfico minorista en zonas, lugares y locales de ocio", y de otro, incorporar la problemática reciente detectada relacionada el incremento de las infracciones y delitos cometidos contra las personas, en zonas, lugares y locales de ocio.

Este Plan de Servicio se prefigura como un "instrumento de choque" en las zonas, lugares y locales de ocio dentro de la demarcación de la Guardia Civil, al objeto de prevenir o evitar el tráfico minorista de drogas, su tenencia y consumo, la comisión de otros actos ilícitos vinculados a la casuística y atenuar la sensación subjetiva de inseguridad que ello provoca en la percepción general de la población. Asimismo, se deben realizar los esfuerzos necesarios para reducir los actos violentos mediante el uso de armas u objetos peligrosos.

Al objeto de la consecución de los fines previstos, se llevarán a cabo, entre otras, impulsar la participación ciudadana y fomentar la colaboración con los empresarios del sector, **así como del personal perteneciente a las empresas de seguridad privada, con quienes se mantendrán entrevistas periódicas y frecuentes.**

Se observarán especialmente las infracciones relativas al consumo o la tenencia ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas en lugares, vías o establecimientos públicos, así como el abandono de los instrumentos u otros efectos empleados para ello en los citados lugares. La ejecución de actos de plantación y cultivo

ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas en lugares visibles al público. La tolerancia del consumo ilegal o el tráfico de drogas tóxicas, estupefacientes o sustancias psicotrópicas en locales o establecimientos públicos o la falta de diligencia en orden a impedirlos por parte de los propietarios, administradores o encargados de los mismos o el porte o uso ilegal, en vías, lugares y establecimientos públicos, de armas, explosivos, sustancias peligrosas u otros objetos, instrumentos o medios que generen un riesgo potencialmente grave para las personas, susceptibles de ser utilizados para la comisión de un delito o alterar la seguridad ciudadana.

COORDINACIÓN

Se promoverá la colaboración de los empresarios de la industria del ocio y el sector de seguridad privada del entorno, mediante el mantenimiento de entrevistas periódicas con los mismos. A tal efecto, se tendrán en cuenta las acciones realizadas por las Unidades en el marco del Programa COOPERA, incentivando las relaciones operativas de las mismas con los departamentos y empresas de seguridad.

Orden de Servicio "Plan ocio seguro", número 13/2023 - MOP GC

3. NOTICIAS DE INTERÉS

3.1 Entrevista a la Capitán Mariluz, del Seprose

El Observatorio Mujer y Seguridad, una iniciativa para visibilizar e impulsar el papel de las mujeres en el ámbito de la seguridad, se hizo eco de la incorporación de la Capitán Dª Mariluz Pérez González a la Sección de Gestión de la Seguridad Privada del Servicio de Protección y Seguridad (SEPROSE). Se adjunta la entrevista.

mujeryseguridad.es/2023/02/06/capitan-mariluz-perez-gonzalez/

Capitán Mariluz Pérez González

SEPROSE

¿Cómo llegó al mundo de la seguridad y cómo llegó al cargo que ocupa actualmente?

Hace 24 años que el toque de diana en la Academia de Guardias cambió el rumbo de mi vida para siempre. El proceso que culmina con mi incorporación al Benemérito Cuerpo está cimentado en una profunda vocación, ya que ser Guardia Civil es un sentimiento, una forma de vida y una manera de ver las cosas que compartimos los que formamos, de alguna manera, parte de esta gran familia. Y eso es extrapolable a todos los que nos dedicamos a la Seguridad, ya sea en el ámbito público como en el privado.

Desde que tengo recuerdos he querido ser Guardia Civil. El porqué de esta decisión prematura, pero que ha sido crucial en mi vida, es la concordancia de valores con el Instituto armado: sacrificio, integridad, profesionalidad, imparcialidad, compromiso, disciplina, abnegación, lealtad y compañerismo, son valores que rigen la actuación diaria de un Guardia Civil y considero imprescindibles para cualquier profesional que forme parte de la Seguridad. He intentado en todos estos años cumplir fielmente con estos valores en cada Unidad en la que he estado.

En cuanto terminé mis estudios y prácticas de Magisterio opositè para el Cuerpo. Siendo ya Guardia Civil me interesé por dos especialidades en concreto, piloto de helicópteros y desactivador de explosivos. Eran un reto para mí, en un momento en el que la presencia de la mujer era mínima en estos puestos (solo había una mujer desactivador y una mujer piloto en esa época). Pero eso no me detuvo, consiguiendo mi objetivo, aunque el camino no fuera nada fácil.

Actualmente formo parte del Servicio de Protección y Seguridad (SEPROSE), perteneciente a la Jefatura de Armas, explosivos y Seguridad de la Guardia Civil (JAES), llevando a cabo las comunicaciones operativas con las Empresas de Seguridad Privada y Departamentos de Seguridad de las mismas, en el ámbito de responsabilidad de la Guardia Civil y de los Programas COOPERA y PLUS ULTRA, así como la tramitación necesaria para la cesión de imágenes de videovigilancia, compaginando estas funciones con otras responsabilidades derivadas de mi empleo.

¿Cómo es tu día a día en el cargo?

La responsabilidad que he adquirido con este nuevo destino es la obligación como profesional dedicada a la seguridad en su más vasto significado. Responder por los propios actos en este campo es básico pero

también hay que responsabilizarse por la imagen corporativa como representante de la Guardia Civil en el ámbito de la seguridad privada, siempre actuando con libertad, voluntad, vocación e inteligencia.

La relación profesional establecida con las empresas, siempre en el marco de mi formación como Director de Seguridad y con los años que me ha dado la experiencia en el sector, posibilitan la asistencia a las mismas en sus más diversas necesidades, adaptando la respuesta a sus objetivos y expectativas, estableciendo una base de colaboración altamente fértil y productiva para ambas partes, todo ello en beneficio de la seguridad y de las buenas relaciones entre el sector público y privado.

La experiencia está siendo altamente gratificante a nivel personal y como profesional en este campo, teniendo en cuenta que, aunque se haya establecido una base estable de comunicación y colaboración, todavía queda mucho camino por andar.

¿Cómo ves la seguridad actualmente?

La seguridad es uno de los mayores objetivos para el desarrollo y el progreso a nivel global.

La inversión económica estaba condicionada por la máxima "lo que no se ve no existe". Esta visión organoléptica del concepto de seguridad impedía ver el alcance y consecuencias de una mala gestión en la materia. Con los nuevos desafíos delincuenciales, sobre todo en el ámbito de la ciberdelincuencia, hemos transformado esa máxima por "lo barato sale caro", contrastada dolorosamente a nivel financiero. Hemos interiorizado como fundamento esencial la comprensión de la importancia de la seguridad como garantía de estabilidad de los poderes e instituciones y de la sociedad en general, siendo esta última ente destinatario de los beneficios de conceder al sector la consideración que se merece. En los últimos tiempos, ha habido una transición en la manera de abordar la seguridad en el ámbito empresarial. Este cambio de estrategia proviene de la necesidad de reajuste a las singularidades de los riesgos y amenazas a los que nos enfrentamos actualmente, en un mundo cambiante y cada vez más digitalizado. Concretamente, una estrategia orientada a una mayor y mejor inversión en seguridad, fortaleciendo los recursos implicados, y desarrollando procedimientos que permitan una utilización de los mismos de forma flexible y eficaz, simultánea a la acción de organismos nacionales e internacionales en materia de regulación del sector, ejerce una sinergia, un impulso que potencia el entendimiento de la repercusión que el abandono de la seguridad tiene en el funcionamiento del tejido empresarial y las instituciones, en tanto que los riesgos y amenazas reales y potenciales no son estancos y, por tanto, no se les puede dar respuestas aisladas. Este criterio solo es posible desde la conjunción del ámbito público y privado. Lo expuesto anteriormente es la diferencia más notoria para mí en la evolución del sector en estos últimos tiempos.

¿Cuáles considera que son los retos de futuro en seguridad?

Como he comentado anteriormente la respuesta a los riesgos y amenazas que actualmente exponen la seguridad necesita de cooperación tanto en el plano nacional como en el internacional. Las respuestas aisladas no son eficaces, por su sesgo y parcialidad, manteniendo mi idea de una perspectiva multidisciplinar.

El ciberespacio es un nuevo ámbito de desarrollo que ha proporcionado la evolución de las tecnologías de la información. La facilidad de acceso, de ocultación de indicios, rapidez de acción y mínimo coste en la ejecución del ilícito, lo convierten en el instrumento de agresión y ejecución criminal preferido. Los ciberataques, han proliferado exponencialmente en el ámbito empresarial y particular debido a una mayor

interconexión digital a nivel global. Esta situación determina la necesidad de priorizar la seguridad de los sistemas con carácter perentorio.

Los cibercriminales llevan a cabo distintas técnicas con diferentes fines, aunque los ataques que registran mayores porcentajes de actuación son las amenazas, el descubrimiento y la revelación de secretos, y los ataques informáticos con matices económicos. El peligro reside en su carácter interdisciplinar, afectando a otros ámbitos empresariales claramente interrelacionados y, generando riesgos que, por su magnitud, son difíciles de atajar.

La vulnerabilidad del ciberespacio observada en los últimos tiempos ha sido objeto de atención prioritaria a nivel global. En los últimos años los ciberdelitos se han desarrollado vertiginosamente, se han sofisticado y especializado, adaptándose a los nuevos usos y tecnologías. Es una tendencia que no solo se mantendrá a corto plazo, sino que irá en aumento de manera exponencial. En breve tiempo los ataques individuales, que tenían motivaciones económicas o de reconocimiento, han sido eclipsados por un modelo de negocio ilegal en el que un grupo de criminales profesionalizados ejercen sus acciones u ofrecen sus servicios a cambio de dinero.

Otro reto a tener en cuenta es la proliferación de grupos radicales y terroristas, totalmente globalizados, con conexiones internacionales y relativa facilidad de acceso a precursores de sustancias químicas, biológicas, deflagrantes, incendiarias y materiales radiológicos o nucleares. El estudio de la materialización de una agresión requiere para su prevención y neutralización un desarrollo normativo y una implicación a nivel mundial.

Otro aspecto a citar son los riesgos y catástrofes derivados de fenómenos naturales, con un gran número de bajas humanas, de pérdidas materiales y que involucran a la mayor parte de los servicios de primera respuesta y emergencia, en un corto espacio de tiempo. Considerar también que estos fenómenos pueden ser promovidos por la acción humana, por lo que es importante incidir en su prevención, diagnosis y evaluación de consecuencias.

¿Qué aporta la mujer a la seguridad?

En general, la incorporación de la mujer al mercado laboral ha ocasionado una transformación del modelo social, familiar y económico. El porcentaje de mujeres en ambientes laborales, roles y puestos de trabajo tradicionalmente masculinos ha facilitado un cambio de mentalidad a nivel general. Los hombres, por costumbre han asumido un rol de protección, fortaleza, independencia y dirección. Nuestro sector presenta una dificultad añadida, relacionado en parte con esta división de roles. El esfuerzo social y legislativo para remover los obstáculos que han impedido la incorporación de la mujer a las diferentes esferas, entre ellas la de seguridad, han dado sus frutos.

Teniendo en cuenta lo expuesto y, bajo un punto de vista general, la incorporación de la mujer, gracias a la remoción del sesgo de género, contribuye al acceso del mejor talento disponible sin discriminación alguna, a una mayor productividad e innovación, ya que la diversidad de genero hace que los equipos sean más creativos y mejora la comunicación y la iniciativa, incrementando la productividad y aportando un punto de vista diferente, lo que optimiza la toma de decisiones.

Este año se celebra el 35º aniversario de la incorporación de las mujeres a la Guardia Civil (1988), considerando, en la actualidad, una necesidad elevar el número de éstas en el Cuerpo, ya que existe un déficit

operativo de plantilla femenina. Este déficit supone una problemática a la hora de abordar y diseñar determinados servicios al ciudadano.

Gracias a las medidas implementadas y al progresivo cambio de mentalidad, las mujeres estamos alcanzando puestos directivos de la máxima categoría, disminuyendo el "techo de cristal" e incorporándonos, como es mi caso, a especialidades tradicionalmente asignadas a roles masculinos, demostrando una vez más que, convenientemente instruidas y formadas, somos completamente eficaces a nivel operativo.

Aunque en los últimos tiempos hemos conseguido grandes avances en la materia, todavía queda mucho camino por andar para evitar que las mujeres tengan que soportar un sobreesfuerzo, debido a la conciliación de la vida familiar y profesional.

3.2 Desarticulada una organización criminal por estafar a más de 3.000 personas en diferentes países con criptomonedas inexistentes.

La Guardia Civil en el marco de la operación "MANDOA", desarrollada en el País Vasco y Baleares, ha procedido a la detención de una persona, vecino de Baleares, con motivo de la investigación de otras cinco personas como autores de una estafa a nivel mundial a través de inversiones en criptomonedas, en la que habrían estafado más de 100 millones de euros a más de 3.000 personas en diferentes países.

La investigación se inició, tras la denuncia de una persona en la provincia de Álava en el que manifestaba haber sido víctima de una estafa por invertir en criptomonedas. Por tal motivo, los agentes procedieron a seguir el rastro de las transferencias de dinero dando como destinatario una empresa que estaba ubicada en Palma de Mallorca.

Continuando con las investigaciones, los agentes pudieron constatar que esta empresa volvía a realizar nuevas transferencias a países ubicados fuera de la Unión Europea, destino final del dinero.

Asimismo, la Guardia Civil pudo averiguar que los miembros de la organización captaban potenciales clientes a través de estrategias de marketing agresivas en conocidas páginas web, mediante llamadas telefónicas, anuncios publicitarios en periódicos, SMS, etc. Y en los que les prometían altos rendimientos sin riesgo.

Una vez que la organización formalizaba el contrato con sus víctimas para realizar las inversiones en criptomonedas inexistentes, que normalmente oscilaban entre los 250 y 1000 euros, la organización les facilitaba un acceso a una página web donde se podían consultar los beneficios de su inversión con falsos gráficos creados al efecto. De este modo, daban una apariencia legal a las operaciones generando así la confianza de las víctimas

Esta operación ha permitido destapar la trama y localizar a las víctimas, 100 de ellas ubicadas en territorio nacional. Cabe destacar que la gran mayoría desconocía que estaban siendo estafadas.

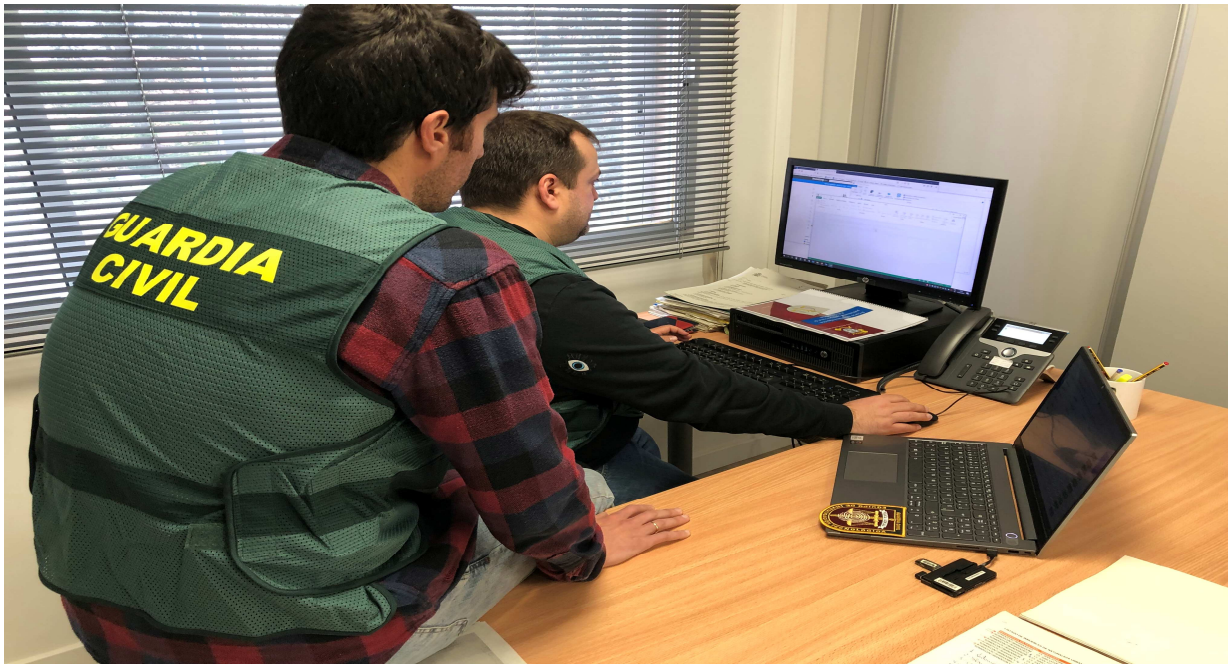
Recomendaciones

En febrero de 2021 la Comisión Nacional del Mercado de Valores y el Banco de España "*advirtieron sobre el riesgo de las inversiones en criptomonedas por su extrema volatilidad, complejidad y falta de transparencia, que las convierte en una apuesta de alto riesgo*".

Por tal motivo debemos desconfiar de las promesas de obtener un gran beneficio o un rendimiento garantizado sin ningún tipo de riesgo y de las ofertas de inversiones que se reciban desde internet en tu correo electrónico o tu teléfono sin haberlas solicitado.

También se aconseja investigar un poco antes de invertir, buscar opiniones y reputación de las webs antes de realizar inversiones, desconfiar de páginas de reciente creación, revisar la dirección ya que a menudo contiene errores ortográficos y no hacer aportaciones en plataformas que tengan la sede social en paraísos fiscales.

Si a pesar de estos riesgos, se desea realizar este tipo de inversión, se recomienda contactar con los organismos oficiales reguladores y consultar sus publicaciones sobre Webs que operan irregularmente.



3.3 La Directora General de la Guardia Civil, Mercedes González, preside la Conferencia de Cooperación Policial con los cuerpos policiales europeos de naturaleza militar.

La Directora General de la Guardia Civil, Mercedes González, preside la Conferencia de Alto Nivel de los directores y comandantes generales de la Gendarmería Nacional Francesa, Arma de Carabinieri de Italia, Guarda Nacional Republicana de Portugal y Guardia Civil que se está desarrollando en la sede del Cuerpo en Sevilla.

Mercedes González ha destacado en la inauguración la importancia de esta iniciativa denominada G4 que se puso en marcha en 2022 en Vicenza (Italia) con los objetivos de compartir experiencias para abordar conjuntamente asuntos relacionados con las amenazas globales, procedimientos preventivos y de investigación y desarrollo de buenas prácticas que contribuyan a comprender y actuar mejor en el mundo que nos rodea haciéndolo más seguro para nuestros conciudadanos.

La Directora General ha anunciado que, a iniciativa de la Guardia Civil se ha creado un nuevo grupo de trabajo de protección del patrimonio histórico y cultural, ya que España es un país líder en diversidad de Patrimonio, siendo el segundo país del mundo y primero de Europa, con mayor número de bienes inscritos en las listas de patrimonio de la UNESCO.

Este grupo refrendará el compromiso e impulso decidido de la Guardia Civil en situar a los principales cuerpos policiales europeos de naturaleza militar en la punta de lanza frente nuevos retos y amenazas, encontrando soluciones válidas y proponiendo estrategias comunes.

En este sentido Mercedes González ha indicado que “es importante la preservación del inmenso patrimonio histórico y cultural, así como en su incalculable valor, no solamente como bien merecedor de una especial protección por la humanidad, sino como eje fundamental en el motor de nuestras economías, nos obliga a ser proactivos en su protección desde una perspectiva integral aunando esfuerzos y compartiendo conocimientos, procedimientos y técnicas en la prevención e investigación”.

Asimismo durante la reunión se han analizado las actividades realizadas en cada uno de los restantes grupos de trabajo que se definieron en la puesta en marcha de esta iniciativa G4 que versan sobre formación conjunta, medio ambiente en el que se ha puesto en marcha una actividad de formación conjunta para el próximo mes de julio; el tercer grupo que trata de ciberdelincuencia, donde se ha hecho hincapié en las propuestas desarrolladas sobre la red de contactos especialistas en ámbito ciber y la celebración de foros multinivel. Para concluir esta reunión G4 Mercedes González ha destacado que este grupo de instituciones policiales con estatuto militar constituye un auténtico núcleo duro en el mantenimiento de una sociedad justa, segura e igualitaria, atento a devenir de los acontecimientos, circunstancias y amenazas claramente detectadas por nuestros expertos y comunes en toda la UE y en su nuevo concepto de Brújula Estratégica.

3.4 Desmantelado un laboratorio clandestino de fabricación de explosivos en Navarra

La Guardia Civil y la Policía Foral de Navarra, en una operación conjunta denominada “ARQUÍMEDES”, han desmantelado, en la localidad de la Cuenca de Pamplona (Navarra), un laboratorio clandestino de fabricación de explosivos a partir de la síntesis de sustancias precursoras de explosivos.

La operación se inició a raíz de la detención de una persona por un episodio de malos tratos en el ámbito familiar. Como consecuencia de la detención los agentes pudieron constatar un posible delito de fabricación ilegal y depósito de sustancias explosivas de esta persona.

Por tal motivo, se procedió al registro del domicilio del detenido donde se halló un laboratorio clandestino con todos los elementos necesarios para la fabricación de explosivos, tales como sustancias precursoras de explosivos, otros productos químicos también utilizados para su fabricación, además de pequeños artefactos explosivos ya terminados, cerillas eléctricas (detonadores), fórmulas químicas e instrucciones y material de laboratorio para la síntesis de los explosivos (pipetas, matraces, termómetros y vasos de precipitado).

Cabe destacar que, con los productos incautados en el laboratorio clandestino, se podrían haber elaborado explosivos artesanales como, triperóxido de triacetona (TATP), amonal, pólvora negra y termita todos ellos muy peligrosos y de alto poder destructivo, destaca por su

peligrosidad el TATP (Triperóxido de Triacetona), también conocido como la “Madre de Satán”, explosivo habitualmente utilizado por grupos terroristas islamistas.

Igualmente, se ha logrado identificar los establecimientos que, de forma indebida, han vendido los precursores de explosivos al detenido. Los precursores de explosivos son sustancias químicas que, a partir de determinadas concentraciones y mezcladas entre sí o con otros productos, son susceptibles de utilizarse para la fabricación casera e ilícita de explosivos, por lo que su comercio, adquisición, tenencia y uso están rigurosamente regulado. En España para su adquisición es necesaria una Licencia que otorga el Ministerio del Interior a través del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), que es el Punto de Contacto Nacional en materia de precursores.

Los agentes han podido determinar que el detenido había adquirido los conocimientos necesarios para la fabricación de explosivos de forma autodidacta a través de manuales y vídeo tutoriales descargados de internet.

La investigación ha estado coordinada por el Juzgado de Primera Instancia e Instrucción número Uno de Aoiz (Navarra).

4. EVENTOS.

4.1 Asistencia a TECNOSEC y DRONExpo

TECNOSEC es el evento de seguridad global que ofrece una oportunidad única en clave nacional e internacional para generar contactos y compartir conocimiento sobre los últimos avances en seguridad, inteligencia y resiliencia entre proveedores, técnicos y responsables de la seguridad pública, defensa e infraestructuras críticas.

DRONExpo aspira a convertirse en el referente de los aparatos de vuelo no tripulado, sus desarrollos y aplicaciones. Diseñado a medida de la industria de drones, integrando a todos los actuantes para presentar las novedades del sector, encontrar oportunidades de colaboración entre empresas y administración, estando a la vanguardia en tecnología e información sobre el futuro del vuelo no tripulado.

Ambos eventos se desarrollaron a la par los días 26 y 27 de abril en el Pabellón de Cristal de la Casa de Campo de Madrid y asistieron miembros del SEPROSE.

5. CONVOCATORIAS

5.1 Guardas Rurales y sus especialidades

Resolución de 12 de octubre de 2022, de la Secretaría de Estado de Seguridad, por la que se aprueban, para el año 2023, el calendario y las bases de las convocatorias de las pruebas de selección para Guardas Rurales y sus especialidades.

Período de presentación de instancias:

Convocatoria 1/2023: Plazo finalizado.

Convocatoria 2/2023: del 01 al 30 de septiembre de 2023, ambos inclusive.

https://www.guardiacivil.es/es/servicios/tablonanuncios/guacampo/index.html