

COVID-19 EN LA GUARDIA CIVIL: LA TECNOLOGÍA COMO ESTRATEGIA DE RESPUESTA RÁPIDA FRENTE A LA PANDEMIA

JESÚS SALVADOR CANO CARRILLO

CAPITÁN Y DOCTOR EN INGENIERÍA
JEFATURA DE SERVICIOS TÉCNICOS DE LA GUARDIA CIVIL

RESUMEN

COVID-19 ha supuesto una tragedia social y sanitaria sin precedentes, tanto para la sociedad en su conjunto como para empresas y administraciones públicas, de la que la Guardia Civil no ha quedado indemne. La acelerada coyuntura con la que se han sucedido los acontecimientos tampoco ha dejado indiferente a otros cuerpos policiales. Para la seguridad pública ha sido un reto sin precedentes, de cuyas características adversas e imprevisibles la historia sabrá dar cuenta. Ha puesto a prueba la estructura misma de funcionamiento de la organización con más de 176 años de existencia, cuyo personal ha sabido responder con profesionalidad y dedicación. Ante la situación inédita de velar por el orden impuesto por el gobierno para frenar la pandemia, la plantilla y los cuadros de mando, en permanente disposición para el servicio desde la declaración del Estado de Alarma, sufrieron bajas importantes como víctimas a su vez de los contagios. Este trabajo trata de aportar cómo la Guardia Civil ha enfrentado al coronavirus a través de la tecnología, de forma expedita y satisfactoria, desplegando una estrategia digital inspirada en respuestas rápidas de negocio, desarrollo ágil y teletrabajo sobrevenido a raíz del estado de alarma sanitaria. A la postre, ha permitido mantener el nivel de servicio al ciudadano, en el prácticamente 80% del territorio nacional que corresponde a su ámbito de competencia, además de en áreas especializadas de la Guardia Civil como Policía Judicial, Información, Seguridad Vial, Protección de la Naturaleza o Fiscal y Fronteras.

Palabras clave: COVID-19, tecnología, teletrabajo, desarrollo ágil, estrategia de respuesta rápida, telecomunicaciones, virtualización.

ABSTRACT

COVID-19 has been an unprecedented social and health tragedy, both for society, as a whole, as well as companies and public sector, from which the Civil Guard has not been unscathed. The accelerated conjuncture which the events have occurred with, has not left other police forces indifferent either. For public safety, it has been an unprecedented challenge, whose adverse and unpredictable characteristics history will know how to account for. It has placed a strain on the very operation structure of a 176-year-old organization and its staff had responded with professionalism and dedication. Faced with this unprecedented situation of ensuring the public order imposed by government to stop the pandemic, the workforce and command panels, in permanent readiness for service since the declaration of the State of Alarm, suffered significant casualties as victims of the contagions. This work tries to contribute how the Civil Guard has been responding the coronavirus through technology, in an expeditiously

and satisfactory way, deploying a digital strategy inspired by quick business responses, agile development and teleworking occurred as a result of the Health Alarm State. In the end, it has allowed to maintain the level of citizen service, in practically 80% of the national territory that corresponds to the total scope of its competence, in addition also in specialized material areas of the Civil Guard such as judicial police, intelligence, road safety, protection of nature or borders.

Keywords: COVID-19, technology, telecommuting, agile development, rapid response strategy, telecommunications, virtualization.

1. INTRODUCCIÓN

La expansión de lo que empezó a conocerse como neumonía vírica, a finales del año 2019 en China, asaltó España ya con el nombre técnico de coronavirus SARS-CoV-2, rebautizado como COVID-19 por la Organización Mundial de la Salud (OMS, 2020). Según el Centro Nacional de Epidemiología (CNE) en nuestro país se confirmaron los dos primeros casos a principios de febrero (CNE, 2020). Vertiginosamente, como se muestra en la Figura 1, la evolución de contagios tuvo un impacto extraordinariamente ascendente durante el mes de marzo. Es cuando, precisamente a primeros de marzo, surgen los primeros cuatro casos positivos entre el personal de la Guardia Civil.

Ante este escenario sanitario el Gobierno planteó un primer plan de contingencia de contención reforzada, suspendiendo la actividad educativa desde el día 9 de marzo, lo que precisó de instrucciones específicas por parte de la Dirección General de la Guardia Civil (DGGC). Dichas instrucciones fueron publicadas en la Intranet del Cuerpo para conocimiento general de la plantilla, haciendo expresa mención, por un lado, a las necesidades del servicio y, por otro, a la protección de la salud y la conciliación de la vida profesional y familiar de los miembros del Cuerpo. Además, consecuentemente, se suspende la actividad académica del alumnado de la Academia de Oficiales de Aranjuez (AOGC), Academia de Suboficiales de San Lorenzo del Escorial (ASGC), Colegio de Guardias Jóvenes de Valdemoro y el Centro de Adiestramientos Especiales de Logroño. Continuadamente en el tiempo, el Centro Universitario de la Guardia Civil (CUGC) y la Academia de Guardias Civiles de Baeza se unirían a la suspensión, así como otros centros de enseñanza propios¹. Igualmente se ordena aplazar o suspender las actividades que impliquen un elevado número de personas, como reuniones, el uso de transportes colectivos y la reducción de desplazamientos de personal al extranjero. Como corolario, se plantea, siempre que el servicio lo permita, la posibilidad de establecer un aumento de horas en la jornada, a fin de incrementar los días de descanso, permitir mayor ratio en cuanto a número de agentes simultáneamente de descanso, la posibilidad de ajustar los horarios para facilitar el cuidado de hijos y familiares, así como “se fomentará el teletrabajo en aquellas unidades y tareas que lo permitan” (CUGC, 2020).

1 La Guardia Civil dispone dentro de su sistema de enseñanza de un conjunto de centros para facilitar la formación, el perfeccionamiento y los estudios profesionales necesarios para las distintas actividades que se desempeñan. Inclúyanse adicionalmente: Escuela de Tráfico en Mérida, Escuela de Montaña de Jaca, Escuela de Adiestramiento de perros en El Pardo, Escuela de Especialización y el Centro de Adiestramiento en desactivación de explosivos y NRBQ de Valdemoro.

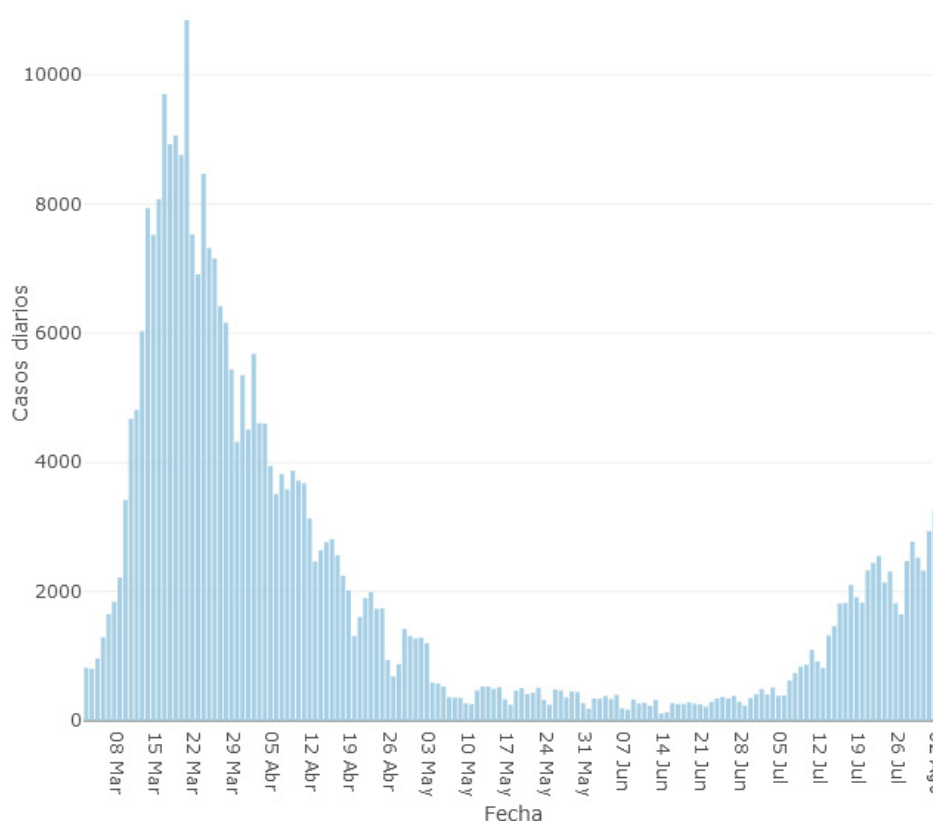


Fig. 1 Curva epidémica general en España (Fuente: CNE).

A estas medidas urgentes y contundentes de por sí, hay que sumar pocos días después la declaración del estado de alarma en todo el territorio nacional, mediante el Real Decreto 463/2020, de 14 de marzo (BOE, 2020a) y sus prórrogas, lo que implicaría un esfuerzo adicional para hacer cumplir con eficacia los mandatos de la nueva situación, garantizar las misiones propias de la Guardia Civil y el servicio a los ciudadanos.

El despliegue territorial de la Guardia Civil, con una cobertura del 80% a nivel nacional, también exigía una diligente respuesta en núcleos urbanos de su demarcación, zonas rurales, carreteras y poblaciones. La Guardia Civil ha desempeñado su labor priorizando el apoyo a la atención y gestión sanitaria, siguiendo la Orden INT/226/2020, de 15 de marzo (BOE, 2020b), manteniendo el orden público y auxiliando en el abastecimiento de elementos de primera necesidad y situaciones de precariedad, de cuyos recuerdos de gratitud además han sido testigos las redes sociales y medios de comunicación. Entre ellas, más de 50.000 servicios humanitarios, como reparto de comida y medicamentos a los colectivos más vulnerables, personas de avanzada edad o que se encontraban solas, entrega de material médico y material escolar en entornos rurales, colaboración para la instalación de hospitales de campaña y tiendas modulares para hacer pruebas de COVID-19, traslado de material médico como respiradores para centros hospitalarios y apoyo en operaciones para trasplantes (ORIS, 2020a).

Los datos durante el estado de alarma dan fe de este trabajo: 22.700 reuniones para conocer la situación de las residencias de mayores, 22.000 a centros sanitarios, 800 actuaciones de desinfección de instalaciones con equipos NRBQ. Para atender la problemática de la violencia de género durante el confinamiento, la Guardia Civil ha

tenido especial dedicación con el seguimiento de 23.000 víctimas con las que se ha mantenido un estrecho contacto, que se ha concretado en: unas 91.000 actuaciones, 3.000 denuncias y 4.000 detenidos por estos hechos. En el ámbito cibercriminal, se han recibido 13.000 comunicaciones de estafas online, que los ciberdelincuentes han aprovechado particularmente durante este período de pandemia. En líneas generales, con los datos obtenidos durante el confinamiento general², han sido alrededor de 900.000 dispositivos de seguridad, donde se ha identificado a más de 10 millones de personas y 8 millones de vehículos, 300.000 denuncias y 170.000 desplazamientos injustificados (ORIS, 2020b).

En lo que sigue, este trabajo trata sobre el esfuerzo tecnológico sobrevenido, que en definitiva ha facilitado y ha podido hacer efectivo el valor operativo de la Guardia Civil. La puesta en marcha de una transformación digital de respuesta rápida, desplegando una serie de plataformas y sistemas de información para acceso remoto, ha permitido mitigar el impacto de la pandemia sobre el personal propio y una razonable continuidad del servicio público que tiene la institución encomendada constitucionalmente.

2. PROBLEMÁTICA COVID-19

Considerando que la Guardia Civil es el cuerpo policial de mayor envergadura en España y posiblemente en Europa, las medidas organizativas orientadas a evitar la propagación del virus en las dependencias oficiales, entre sus cerca de 80.000 miembros, no eran tarea baladí. Más si cabe cuando siguiendo la normativa vigente, en caso de la declaración del estado de alarma, todo el personal uniformado se activa quedando a disposición inmediata de sus mandos y dejando en suspenso los permisos y períodos vacacionales. Como consecuencia, la disponibilidad de la mayor plantilla en revista posible supone un potencial pleno de la fuerza, a disposición de las necesidades del Estado para hacer frente a la pandemia.

Ante la inevitable concentración de componentes del Cuerpo, imprescindible para atender las tareas que los guardias civiles tienen a diario y las extraordinarias provocada por la crisis, se hace necesario prevenir el adecuado potencial en servicio, toda vez que se comienza a detectar los primeros casos entre el personal, en algunas dependencias, afectando incluso de forma crítica.

Las primeras indicaciones, como forma de proceder en caso de contagio positivo o de síntomas durante el servicio, se dieron con la Orden de Servicio número 19/2020, informando al escalón médico de su unidad y procediendo a la atención sanitaria correspondiente de su comunidad autónoma. Al objeto de establecer un adecuado sistema de transmisión de novedades, para facilitar la posible necesidad de información extraordinaria, siguieron la Orden de Servicio número 20/2020 y, posteriormente, la Orden de Servicio número 21/2020 para, de forma organizada, tener unas pautas básicas de actuación para la transición a la nueva normalidad.

La realidad es que la curva epidémica en el colectivo de la Guardia Civil se dispara desde mediados del mes de marzo, como puede verse en la gráfica superior de la

2 Téngase en cuenta que se trata del balance hecho de alrededor de tres meses de estado de alarma, desde marzo a junio, período donde se ha realizado el mayor esfuerzo por parte del Instituto Armado.

Figura 2, representando un total de más de 3.200 casos confirmados y de los que durante esta etapa tristemente hay que contar 9 fallecidos.

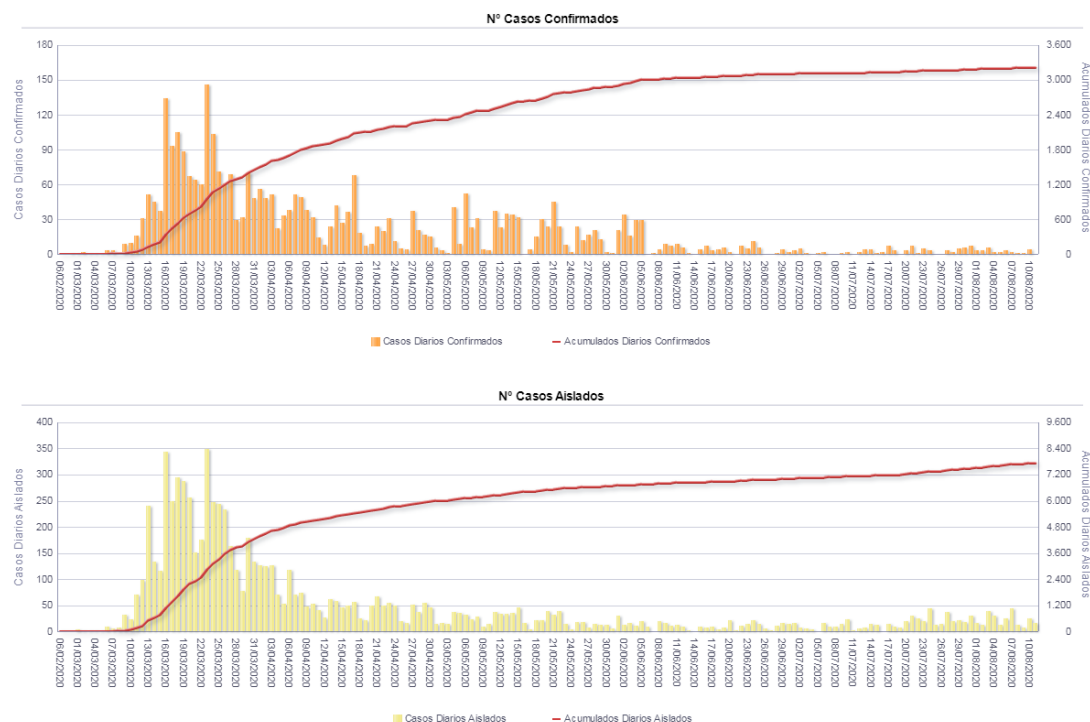


Fig. 2. Curva epidémica en Guardia Civil (arriba) y aislados (abajo).

En este estadio, la parte inferior de la Figura 2 muestra el personal sobre el que se ha determinado el aislamiento sanitario preventivo³. A este colectivo se suma el personal con aislamiento por síntomas compatibles o que había mantenido contacto con alguien contagiado, tanto en su entorno más cercano como en el profesional, o bien personal perteneciente a colectivos vulnerables o con patologías de riesgo, que han supuesto algo más de 7.800 miembros.

3. TELETRABAJO

Hay un consenso general en situar el origen conceptual del teletrabajo en los años 70 (Pérez Sánchez, 2010), particularmente como consecuencia de otra crisis: la Crisis del Petróleo (Maffeo, 2003). En 1973, los países del golfo Pérsico tomaron la decisión de no exportar petróleo a los países occidentales, lo que provocó un impacto económico inmediato y una fuerte inflación. La subida del precio del crudo y el estilo de vida americana, con domicilios retirados y dependencia del coche para acudir al centro de trabajo, provocó barajar la posibilidad de trabajar desde casa. Como menciona Pérez Sánchez (2010), se le atribuye al ingeniero Jack Nilles, considerado padre del teletrabajo, la idea inspiradora de que si uno de cada siete trabajadores

3 Los datos obtenidos han sido posibles gracias al desarrollo informático de Inteligencia de Negocio COVID-19, implementado por el personal técnico de la Jefatura de Servicios Técnicos, a través de su Servicio de Informática, como una de las medidas tecnológicas de carácter excepcional para el control y apoyo a la decisión estratégica del alto mando de la Guardia Civil. Vid. Sección de detalle ut infra.

no se desplazara a su centro de trabajo entonces Estados Unidos no tendría la necesidad de importar petróleo (Nilles, 1975). Modos de razonamiento similares han ido surgiendo, tanto para zonas rurales como urbanas a lo largo de los años como consecuencia, en palabras de Ortiz Chaparro (1999), de la aplicación al mundo laboral de las tecnologías de la información y las comunicaciones (TIC).

3.1. MARCO LEGAL

Uno de los primeros hándicaps que se observó a nivel técnico resultó ser la falta de un marco legal de referencia para implementar un puesto de trabajo de guardia civil en remoto. Si bien en la norma legal de régimen de personal del Cuerpo, publicada en el Boletín Oficial del Estado (BOE, 2014), no encontramos mención alguna al teletrabajo (L. 29/2014, de 28 de noviembre), tampoco lo hallamos en el Estatuto del Empleado Público (BOE, 2015a), salvo en lo referido en este caso a la posibilidad del uso telemático del voto en procesos electorales, enfocado a la elección de representantes de las Juntas de Personal y delegados (R.D.L. 5/2015, de 30 de octubre).

Sin otra concreción mayor, la referencia legal más apropiada en la esfera administrativa sobre teletrabajo (BOE, 2005) la encontramos como resultado de una experiencia piloto del Ministerio de Administraciones Públicas (MAP), en el marco del Plan Concilia (O. APU/3902/2005, de 15 de diciembre). Dicho piloto se realizó tomando de hecho a 30 funcionarios de la subsecretaría del MAP que se prestaron voluntariamente a teletrabajar y cuyo desempeño fue evaluado positivamente por sus jefes de unidad (MAP, 2006). Con ese ánimo surgió la Orden APU/1981/2006, de 21 de junio, para impulsar y difundir la realización de pilotos similares que demostrasen la viabilidad del teletrabajo en otros departamentos ministeriales (BOE, 2006). No obstante, la reproducción de la experiencia no era tarea fácil, ya que la propia orden advertía que la naturaleza de las funciones de los puestos de trabajo iba a ser determinante para embarcarse en el trabajo remoto, presumiendo genéricamente incompatibles algunas posiciones dentro de la Administración General del Estado (AGE), como aquellos que requieran contactos personales frecuentes o atención directa al público:

En todo caso, no podrán ser incluidos aquellos puestos de trabajo que requieran para su adecuado desempeño contactos personales frecuentes o atención directa al público. Condiciones de los empleados que podrán solicitar su participación en el programa piloto, que deberán encontrarse en servicio activo y reunir conocimientos suficientes en ofimática (BOE, 2006: 23775).

A pesar del desierto normativo que rodea la problemática de implantar el trabajo remoto en la Guardia Civil, algo cierto y positivo hemos podido sacar de aquella orden piloto de 2006: una definición de teletrabajo en el ámbito de las administraciones públicas. El apartado primero de la citada orden define teletrabajo como:

Modalidad de prestación de servicios de carácter no presencial en virtud de la cual un empleado de la Administración General del Estado puede desarrollar parte de su jornada laboral mediante el uso de medios telemáticos desde su propio domicilio, siempre que las necesidades del servicio lo permitan y en el marco de la política de conciliación de la vida personal y familiar y laboral de los empleados públicos.

El legislador por otro lado, para el ámbito laboral, incorporó el trabajo a distancia en el Estatuto de los Trabajadores (ET, R. D. L. 2/2015, de 23 de octubre), como “modo alternativo a su desarrollo presencial en el centro de trabajo de la empresa” (BOE, 2015b:19) cuya definición extraída de su artículo 13 ni tan siquiera nombra el

uso de las telecomunicaciones, aunque podemos convenir que puede considerarse inherente en la sociedad actual. De hecho, al trabajador se le dota del derecho a la solicitud del trabajo a distancia, que debe ser negociada con la conveniencia de la empresa (Ferrán Kernel, 2020) y cuya denegación debe estar justificada, como avalan recientes sentencias judiciales y la doctrina al respecto (Sánchez-Urán Azaña, 2019).

Ciertamente, en la conciencia europea ha habido una intención globalizadora, siendo significativo el Acuerdo Marco Europeo sobre Teletrabajo de 2002, donde se pretende equiparar trabajo presencial y trabajo remoto. En la práctica, el acuerdo aspiraba a que el teletrabajo fuera un acicate para la modernización de las empresas y de los servicios públicos, a la vez que pudiera flexibilizar la vida personal y familiar de los trabajadores mediante el uso de las TIC (Belzunegui Eraso, 2008).

A raíz de la emergencia sanitaria, sin embargo, se ha podido comprobar que además de la conciliación, el teletrabajo es un asunto que se ha vuelto clave para la salud pública. Personas con o sin necesidad de conciliar se han visto abocadas al teletrabajo, de la misma manera que las organizaciones lo han abrazado en estos tiempos como medida salvavidas, a pesar de que teletrabajar tiene sus dificultades, ya que no consiste “en simplemente cambiar la ubicación del trabajador” (Mapfre, 2020).

3.2. SITUACIÓN EN LA GUARDIA CIVIL

La premurosa necesidad de no aglomerar personal suponía obviamente iniciar medidas de no disponibilidad en los acuartelamientos, unas veces promovida por el contagio del personal o sus convivientes, otras por aislamientos por motivos preventivos y en otras como medida prudente para, de ser posible, establecer turnidades de presencialidad, que son decididas bajo criterios de eficacia de los mandos correspondientes. Todo ello, en corto espacio de tiempo, ha impactado en la tradicional forma de hacer las cosas en el colectivo de guardias civiles, llegando inicialmente a considerarse dramática en algunas unidades a la vista de la merma de efectivos que, por otro lado, afectó de forma desigual según los sitios. Los servicios centrales, jefaturas y servicios, así como unidades de coordinación periféricas, estuvieron al límite en ocasiones de paralizar su estructura de mando y, por ende, su organización administrativa. La facilidad de la expansión del virus en las dependencias en las que no se hacía posible un distanciamiento mínimo y la incertidumbre generada por no poder predecir la evolución de la pandemia, llegaron a poner a la organización en una situación de extrema preocupación.

Se veía necesario dar continuidad al servicio, para lo que era imprescindible activar a la fuerza desplazada, aislada o en cuarentena, cuya salud y compromisos lo permitiera, tanto por su cuantificación como por la necesidad de dotar de manera segura de alguna herramienta que habilitara el trabajo en grupo y el ejercicio del mando.

Al igual que en otras entidades públicas y privadas, el teletrabajo se anunciaba como una posible alternativa para paliar los efectos de la pandemia, pero que se volvía imprescindible con la capilaridad territorial que presenta el Cuerpo.

La inexcusable misión de la Guardia Civil, cuyas funciones policiales y administrativas son eminentemente colectivas, de trato social y prácticamente inevitable contacto físico en muchas ocasiones, se enfrentaba al reto de practicar una

acelerada adaptación digital hacia el trabajo en remoto. O lo que es más, se trataba de concebir en la Guardia Civil un modelo híbrido de trabajo presencial imbricado en el trabajo telemático que nos sirviera de referencia, para lo que no existían modelos ni experiencia previa similar a seguir. Ante la imprevisibilidad de la evolución sanitaria, que resultaba complicado evaluar, no se disponía, como es comprensible por la situación, de un protocolo operativo o procedimiento de contingencia para un uso generalizado del teletrabajo.

Por la naturaleza de sus funciones, hay que reconocer que desvincular al guardia civil del puesto de trabajo físico tampoco hubiera sido encomienda fácil en situación de normalidad. Pero, el aislamiento fortuito y la cuarentena preventiva inopinada de cualquier miembro, requería con urgencia la ubicuidad del puesto de trabajo para acceder correctamente a la información y a las infraestructuras tecnológicas propias de un entorno de ciberseguridad crítica, como estudia Cano y Hernández (2017), al manejar asuntos policiales y judiciales de transcendencia. Surge, con las primeras bajas, el imperativo de coordinar un potencial mínimo en los cuarteles por vía telemática que, además de facilitar la flexibilidad horaria, pueda poner en contacto a los desplegados remotamente como si formaran parte de la infraestructura del Cuerpo. La Guardia Civil se llevaría electrónicamente el cuartelillo al lugar de confinamiento, o al menos en parte, en un sentido expresivo de tratar de trasladar la actividad de la casa-cuartel al cuartel en casa.

Todo ello se concretó en poner en marcha una respuesta tecnológica como estrategia rápida, con la inmediata actuación de los recursos disponibles en la Jefatura de Servicios Técnicos (JST), ya que se necesitaba empujar en la misma dirección y acertar, tanto en el ámbito estrictamente informático, a través del Servicio de Informática (SINF), como en el ámbito de las comunicaciones a cargo del Servicio de Telecomunicaciones (STEL), asegurando el tratamiento de los datos de criminalidad recabados de todas las unidades del Cuerpo a través del Servicio de Estadística. Además, junto con el Servicio de Criminalística, se iniciaron los trabajos para formar un consorcio con otros institutos forenses europeos e investigadores expertos en la adaptación y optimización de pipelines bioinformáticos. Con ello, el Servicio de Innovación Tecnológica y Seguridad de la Información, dependiente de la JST, por su parte, trata de contribuir en la experiencia tecnológica en secuenciación de tercera generación de ADN y agentes biológicos, como son los virus, en escenarios de interés con recogida de muestras “in situ” que permitan obtener resultados rápidamente.

La crisis por la irrupción de COVID-19 ha suscitado numerosas cuestiones relacionadas con el acceso y utilización de datos personales de salud, de lo que se ha estado ocupando la reciente Oficina del Delegado de Protección de Datos (DPD) de la JST, para velar por el estricto cumplimiento de los derechos fundamentales reconocidos en nuestra Constitución, en cualquier momento. Al amparo del artículo 18.4 CE, así como la jurisprudencia constitucional relacionada, como resulta la obligada sentencia 292/2000 de 30 de noviembre del Tribunal Constitucional, desde mayo de 2018 se exigía a las Administraciones Públicas una figura expresa y proactivamente supervisora del cumplimiento normativo. En este sentido, se ha asesorado sobre los procedimientos de recogida de datos y comunicación a las distintas partes implicadas, así como aconsejado en las reuniones de gestión de crisis que se han ido desarrollando durante el Estado de Alarma, y posteriormente. Aproximadamente, se han atendido

de forma personalizada durante este período de estudio unas 1.000 consultas vía correo electrónico relacionadas con las restricciones en el libre desplazamiento de la ciudadanía, normativa a cumplir y forma de tramitar la documentación ante la Guardia Civil, que se suman a las tareas ya propias de solicitudes del ejercicio de derechos y reclamaciones por parte de los ciudadanos.

La implantación de mecanismos especiales de ciberseguridad para constituir un entorno controlado y securizado se aventuraba, como así fue, minucioso y laborioso, pero imprescindible para garantizar la normalidad del trabajo operativo en una situación que, obviamente, se iba volviendo descabellado en plena curva de contagios.

Inmediatamente, se planteó la necesidad de identificar los cometidos y funciones seleccionables para continuar el servicio mediante teletrabajo. Era preciso, al menos lo suficiente, para que a nivel técnico se pudiera diseñar una serie de roles suficientes que permitiera ofrecer un escritorio virtualizado del puesto de trabajo que debía montarse en casa. La propia regulación de especialidades del Cuerpo (O. PCM/509/2020, de 3 de junio), con más de una veintena de categorías de especialistas, sin contar otras derivadas, hace una idea de la complejidad de la situación a la hora de ajustar los perfiles y que refleja la importancia que la tecnología tiene en la conciencia de la Institución como capacidad adaptativa:

El desarrollo de las funciones asignadas en un entorno de seguridad en permanente dinamismo, caracterizado por su volatilidad y complejidad, debido a dinámicas como el ritmo acelerado de transformación impulsado por la tecnología, impone que la Guardia Civil deba disponer de la capacidad de adaptación necesaria para poder ofrecer una respuesta eficaz a las amenazas y desafíos a la seguridad. (BOE, 2020c: 38801).

Sin obviar la complejidad de la estratificación del trabajo en la Institución, que trasciende a lo meramente técnico, como se afirmaba ya años atrás con la citada experiencia piloto de la AGE (BOE, 2006), una respuesta rápida exigía una combinación de eficiencia y eficacia tecnológica que debía sacar, con un mínimo de escritorios virtuales, un puesto de teletrabajo con mecanismos seguros, cifrado, autenticación robusta, autorización y control en tiempo real.

4. ESTRATEGIA TECNOLÓGICA

El apoyo tecnológico exigido para la continuidad del servicio operativo en la Guardia Civil requería una estrategia decidida, que se materializara en el cambio en la ingeniería, centrándose en las necesidades sobrevenidas y la reducción de tiempos de respuesta de todas las unidades implicadas en la Jefatura de Servicios Técnicos. Así, se tomaron medidas drásticas para asegurar la disponibilidad del personal técnico, cuadros de mando e ingenieros, manteniendo una coordinación presencial en la sede central de la Jefatura, lo que va en la línea de garantizar la seguridad propia para poder estar en disposición de ayudar al resto de la organización. Esto supuso además la decisión de trasladar a las empresas de tecnología que dan soporte especializado al Cuerpo, incluyendo programadores informáticos, técnicos de redes, administradores de sistemas y otros expertos.

Seguidamente, se articula una estrategia en paralelo que debía confluir en una solución a corto plazo para dar respuesta al posible e imprevisible confinamiento de miles de guardias civiles. Dicha estrategia consistió en lanzar una serie de acciones

de mando de alto nivel, convertidos en proyectos que han supuesto la movilización de todo el personal técnico por su gran impacto y envergadura tecnológica:

- P1: Implantar un sistema informático de escritorio virtual de trabajo, con prestaciones suficientes para perfiles operativos. Esto debía permitir el acceso a la web de contenidos de la Intranet corporativa, el acceso al sistema integral de gestión operativa (SIGO), al sistema de investigaciones (SINVES), al sistema de logística (ALFIL), al sistema de recursos humanos (NERHU) y al sistema estadístico de la Guardia Civil (SEGC). Además, la incorporación en remoto de aplicaciones para la gestión de armas y explosivos (SGAE), entre otras.
- P2: Implantar una red de máquinas virtuales de salto que permitiera la gestión y administración remota de cierta infraestructura tecnológica del Cuerpo, para ingenieros, expertos en telecomunicaciones y programadores informáticos. Con ello, se puede tener el respaldo técnico de la infraestructura para tener en cuenta las incidencias en caso de aislamiento, atender el mantenimiento informático de las plataformas y desarrollar otras nuevas que fueran necesarias. De igual manera los administradores de las redes de telecomunicaciones y de ciberseguridad podrían desempeñar su trabajo sin presencia física exclusiva para gestionar los dispositivos y servidores de seguridad.
- P3: Desplegar un entorno de confianza cero (Zero Trust) para la conexión telemática. Esto es, implantar los túneles cifrados (VPN) necesarios para interconectar los equipos de los usuarios remotos al servicio intermedio de virtualización de los puntos anteriores, haciendo uso de autenticación mediante tarjeta criptográfica y doble autenticación mediante teléfono móvil.
- P4: Securitizar el equipo informático del usuario, para lo que se establece una instrucción de registro previo que permita identificar los nombres de usuario, los sistemas operativos, direcciones y datos del teletrabajador para autorizarlo en el sistema de control de acceso. Además de las medidas propias de antivirus local, se incorpora la instalación de un cliente avanzado de protección anti-exploit y anti-malware de última generación, con análisis basado en aprendizaje automático, que pretende correlar posibles ataques no conocidos.
- P5: Desarrollar una aplicación COVID-19 que proporcione inteligencia de negocio, con la urgencia y con los recursos propios disponibles, para el soporte, control y gestión de la situación sanitaria del personal, contagiado, aislado, preventivo y valorado en tiempo real. De esta manera se confecciona una herramienta de apoyo a la decisión del mando, que centraliza y canaliza toda la información relacionada.
- P6: Desplegar soluciones de trabajo colaborativo y reuniones por videoconferencia, en función del nivel de integridad y confidencialidad requerido, en los distintos contextos de trabajo que se plantean en el servicio de la Guardia Civil.
- P7: Establecer un equipo de vigilancia y monitorización de la red, malware y ciber-incidentes, basado en indicadores de compromiso y atendiendo a

las alertas procedentes del Centro Criptológico Nacional (CCN-CERT) y del Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad (CNPIC), así como reportar a la superioridad las novedades relacionadas a efectos de coordinación.

La focalización de los esfuerzos en un objetivo común ha permitido dar una respuesta eficaz, pero ha necesitado del compromiso de cada uno de los guardias civiles y funcionarios que integran las unidades de la Jefatura de Servicios Técnicos. Por un lado, la modernización de los sistemas de telecomunicaciones y ciberseguridad iniciada este año con la contratación en cuatro lotes del Contrato Unificado de Telecomunicaciones ha requerido un esfuerzo y una flexibilización considerable en pleno despegue de este, al objeto de diseñar una serie de actuaciones lógicamente condicionada por la situación. Además, se han activado los mecanismos para la contratación por el procedimiento de emergencia, previsto por el legislador en el artículo 120 de la normativa de contratación pública (L. 9/2017, de 8 de noviembre), un régimen excepcional que implica directamente a la Guardia Civil como Administración pública a la hora de: “actuar de manera inmediata a causa de acontecimientos catastróficos, de situaciones que supongan grave peligro o de necesidades que afecten a la defensa nacional” (BOE, 2017). Como respaldo legal, se tomaron las medidas urgentes para responder económicamente al COVID-19 dispuestas en el artículo 16 del Real Decreto-Ley 7/2020, de 12 de marzo (BOE, 2020d). Principalmente el gasto en este sentido ha consistido en reforzar el mantenimiento de la plataforma de virtualización de escritorios y aplicaciones (~ 95.000 euros). Por otro lado, se ha requerido la adquisición de 300 ordenadores portátiles con pantalla separable (~ 359.000 euros), 700 ordenadores portátiles ultraligeros (~ 542.000 euros).

Entre los resultados reportados por el Área de Seguridad del Servicio de Telecomunicaciones destacan los intentos de ataques cibernéticos que ha sufrido la Institución, que se ha visto duplicada en este periodo. Principalmente hay que mencionar las actividades de hacking agresivo contra los sistemas de correo, amenazas graves de malware y contra servicios de Administración electrónica que se prestan a los ciudadanos. Además, se observa que las herramientas de trabajo remoto han abierto una ventana de oportunidad a los ciberdelincuentes, lo que era previsible por otro lado, ante lo cual se estableció por parte de la Jefatura un planeamiento exigente en cuanto a medidas de defensa en profundidad y minimización de riesgos. alguna de esas medidas ha sido la implantación de herramientas anti-malware y anti-exploit, basadas en tecnología de Inteligencia Artificial, así como el uso de cifrado y redes privadas virtuales, proxificación y sistemas de redes de máquinas de salto a distintos niveles.

En la Figura 3 se puede ver la evolución de ciberamenazas significativas mediante malware/virus con ocasión de la crisis COVID-19 en la Guardia Civil, en cuyo vector de ataque incluye campañas de correo masivo tipo spam (en azul) y ficheros adjuntos maliciosos detectados por los cortafuegos de detección de intrusiones (IPS) y analizados de forma aislada (técnicas de sandbox). Del análisis de los datos, se aprecia un aumento relevante de los casos de Phishing a las cuentas de usuarios de los guardias civiles desde marzo a julio, pero para esta modalidad notablemente durante el mes de junio.

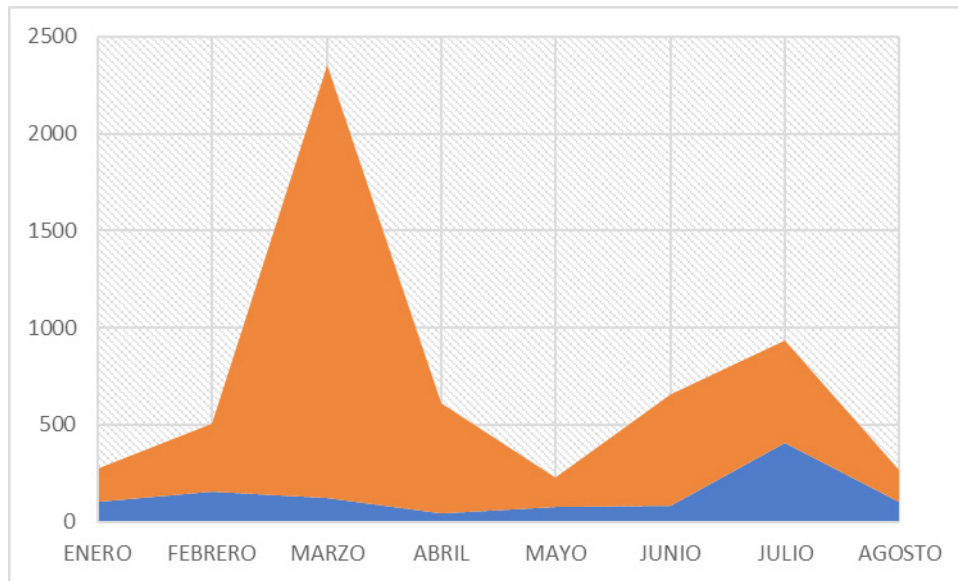


Fig. 3 Malware durante la crisis: adjuntos maliciosos (naranja) y contenido malicioso (azul).

En la Figura 4 se pueden ver los accesos totales de usuarios que han iniciado sesión de trabajo de teletrabajo.



Fig. 4 Teletrabajo total por VPN en Guardia Civil.

Los ataques con códigos maliciosos han sido un hecho importante a repeler, tanto por el Servicio de Telecomunicaciones a nivel perimetral y equipos remotos para teletrabajo desde Internet, como por el Servicio de Informática a nivel de Intranet.

A nivel computacional se ha focalizado el esfuerzo de dotar de herramientas de trabajo peculiares del trabajo policial que desempeña la Guardia Civil a través del diseño e implantación de un portal virtualizado, dentro del paradigma de ciberseguridad de “confianza cero” reforzado con ocasión de la crisis. El uso de escritorios virtuales para teletrabajo ha sido un recurso que han utilizado usuarios finales para poder dar continuidad al servicio, atender las unidades operativas y alcanzar las funciones propias de coordinación policial y atención ciudadana. En la Figura 5 se puede ver la evolución de picos de escritorios virtuales activos diariamente de gestión operativa para este tipo de usuarios en la Guardia Civil.

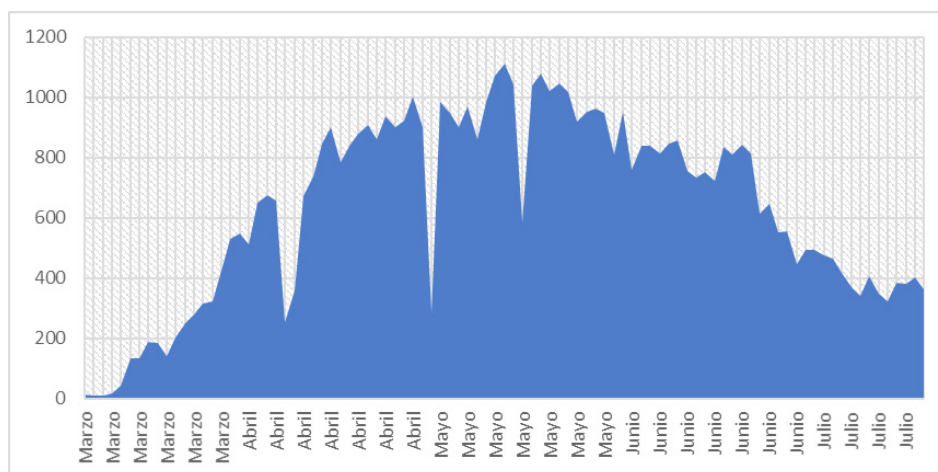


Fig. 5 Escritorios informáticos virtuales implantados para gestión operativa.

El esfuerzo ímprobo de los servicios técnicos se refleja en el apoyo y control de la enfermedad en el colectivo, lo que, como se ha mencionado, supuso el reto de diseñar y desarrollar un sistema de información nuevo, a medida de las específicas necesidades de estrategia de personal, mando y control de la Institución. En esta línea, ha sido fundamental el tratamiento de la información con la aplicación informática desarrollada por la JST, véase por ejemplo, como se muestra en la Figura 6, la gestión de los tests COVID por provincias, arrojando un total de 52.707 miembros de la Guardia Civil controlados, necesitando 67.063 pruebas, tanto PCR como rápidas, que han permitido determinar el grado de afectación positiva del coronavirus con un balance del 6 por ciento de positivos en esta fase de la crisis que ha sido objeto de este estudio.

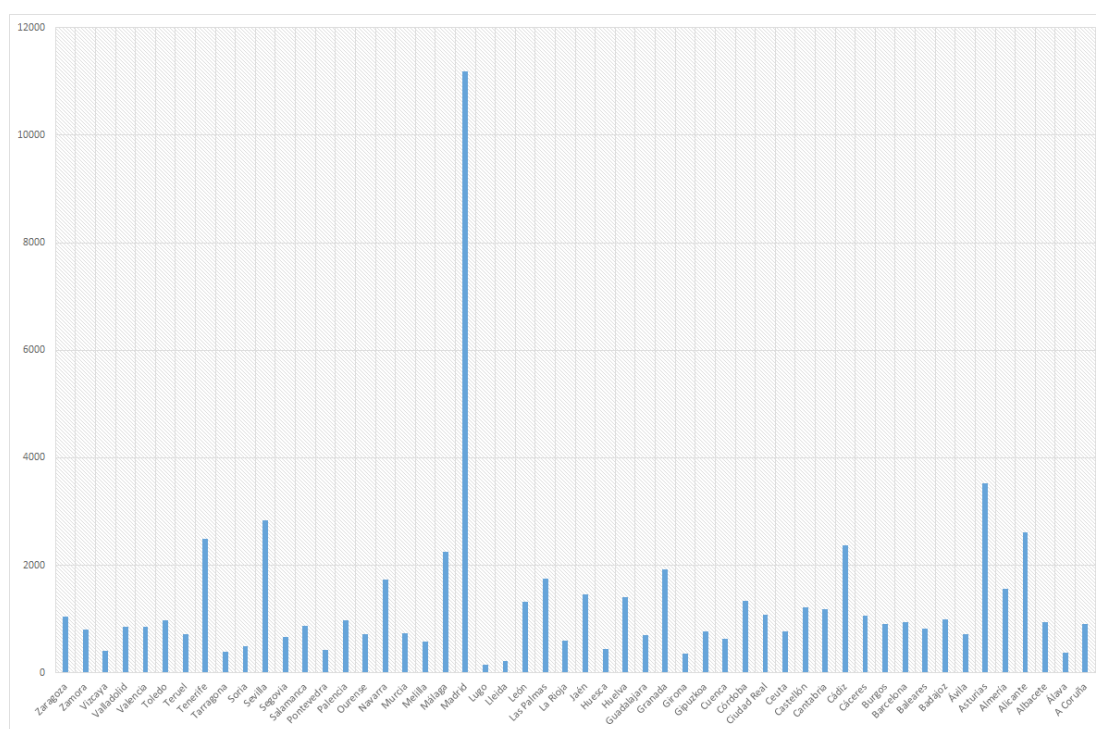


Fig. 6 Datos de tests geolocalizados en la aplicación informática.

5. CONCLUSIONES

La situación de alarma sanitaria ha afectado de forma global, imprevisible y desde múltiples perspectivas, demostrando varios aspectos para tener en cuenta con relación a las unidades que integran la Jefatura de Servicio Técnicos:

Primero, la misión del Cuerpo ha estado bajo niveles de servicio adecuados a las exigencias de la crisis, constituyendo las tecnologías de la información un factor imprescindible para el trabajo operativo, de personal y logístico.

Segundo, la precisión de dar una respuesta rápida, a los retos tecnológicos que plantearon, y la capacidad de adaptación, a escenarios en constante evolución, han supuesto una aceleración en los procesos de digitalización del puesto de trabajo.

Tercero, hay que valorar el esfuerzo estratégico, organizativo y técnico de los implicados en este reto tecnológico, para ejecutar con una respuesta rápida la adaptación necesaria al escenario demandado de seguridad pública y protección de la salud propia.

Cuarto, la habilitación hacia un cambio de paradigma de trabajo, colaborativo y ubicuo, en permanente conexión y con disponibilidad completa a cualquier hora de personal, infraestructuras y servicios.

En esencia, la Guardia Civil ha demostrado su capacidad de adaptación, al haber puesto las tecnologías de la información en el núcleo del proceso de negocio, siendo pieza crucial para afrontar la crisis y la alarma sanitaria en nuestro país.

BIBLIOGRAFÍA

Belzunegui Eraso, A. (2008). Eraso, A. G. B. (2008). Teletrabajo en España: acuerdo marco y Administración Pública. RIO: Revista Internacional de Organizaciones, (1), pp. 129-148.

Cano, J., y Hernández, R. (2017). Managing Software Architecture in Domains of Security-Critical Systems: Multifaceted Collaborative eGovernment Projects. In Securing Government Information and Data in Developing Countries. pp. 1-26. IGI Global.

BOE (2005). Boletín Oficial del Estado. Plan Concilia. Orden APU/3902/2005, de 15 de diciembre, por la que se dispone la publicación del Acuerdo de la Mesa General de Negociación por el que se establecen medidas retributivas y para la mejora de las condiciones de trabajo y la profesionalización de los empleados públicos. BOE núm. 300, de 16 de diciembre de 2005, pp. 41081-41084.

BOE (2006). Boletín Oficial del Estado. Orden APU/1981/2006, de 21 de junio, por la que se promueve la implantación de programas piloto de teletrabajo en los departamentos ministeriales. BOE núm. 149, de 23 de junio de 2006.

BOE (2014). Boletín Oficial del Estado. Ley 29/2014, de 28 de noviembre, de Régimen del Personal de la Guardia Civil. Jefatura del Estado. BOE núm. 289, de 29 de noviembre de 2014.

BOE (2015a). Boletín Oficial del Estado. Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los

Trabajadores. Ministerio de Empleo y Seguridad Social. BOE núm. 255, de 24 de octubre de 2015.

BOE (2015b). Boletín Oficial del Estado. Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. Ministerio de Hacienda y Administraciones Públicas. BOE núm. 261, de 31 de octubre de 2015.

BOE (2017). Boletín Oficial del Estado. Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. BOE núm. 272, de 09 de noviembre de 2017.

BOE (2020a). Boletín Oficial del Estado. Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. BOE núm. 67, de 14 de marzo de 2020.

BOE (2020b). Boletín Oficial del Estado. Orden INT/226/2020, de 15 de marzo, por la que se establecen criterios de actuación para las Fuerzas y Cuerpos de Seguridad en relación con el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. BOE núm. 68, de 15 de marzo de 2020.

BOE (2020c). Boletín Oficial del Estado. Orden PCM/509/2020, de 3 de junio, por la que se regulan las especialidades en la Guardia Civil. BOE núm. 163, de 10 de junio de 2020.

BOE (2020d). Boletín Oficial del Estado. Real Decreto-ley 7/2020, de 12 de marzo, por el que se adoptan medidas urgentes para responder al impacto económico del COVID-19. BOE núm. 65, de 13 de marzo de 2020.

CNE (2020). Primeros casos investigados en España por Covid-2019: Informe Covid-2019 nº 1. 11 de febrero de 2020. Extraído el 1 de agosto de 2020 de: https://www.isciii.es/QueHacemos/Servicios/VigilanciaSaludPublicaRENAVE/EnfermedadesTransmisibles/Documents/INFORMES/Informe_COVID-19_Nº3_28febrero2020_ISCIII.pdf

CUGC (2020). El CUGC continúa su actividad académica en modalidad online. 12 de marzo de 2020. Extraído el 1 de agosto de 2020 de: <https://www.cugc.es/noticias/noticias-por-categoria/actualidad/item/229-el-cugc-continua-su-actividad-academica-en-modalidad-online>.

Ferrán Kernel, M.M. Reconocimiento del derecho al teletrabajo: ¿en qué punto estamos? Expansión, 21 de febrero de 2020. Extraído el 1 de agosto de 2020. Disponible en: <https://www.expansion.com/juridico/opinion/2020/02/21/5e4ed474e5fdea3a568b45e9.html>.

Nilles, J. (1975). Telecommunications and organizational decentralization. IEEE Transactions on Communications, 23(10), pp. 1142-1147. Extraído el 1 de agosto de 2020. Disponible en: <http://adapt.it/adapt-indice-a-z/wp-content/uploads/2017/07/Telecomm-and-Org-Decentralization.pdf>

Maffeo, A. J. (2003). La Guerra de Yom Kippur y la crisis del petróleo de 1973. *Revista Relaciones Internacionales*, 25, pp. 2-6.

MAP (2006). Plan Concilia. Intervención de la Subsecretaria del Ministerio de Administraciones Públicas, Dolores Carrión. Extraído el 1 agosto de 2020 de: http://www.mptfp.es/dam/es/portal/prensa/historico_intervenciones/historico_Jordi_Sevilla/intervenciones/0110/20060307subsecretaria-PlanConc.pdf.

MAPFRE (2020). El teletrabajo como herramienta para la salud pública. Redacción MAPFRE de 16 de marzo de 2020. Extraído el 1 de agosto de 2020. Disponible en: <https://www.mapfre.com/teletrabajo-herramienta-salud-publica>.

OMS (2020). Cronología de la respuesta de la OMS a la COVID-19. Organización Mundial de la Salud. Última actualización: 30 de julio de 2020. Extraído el 1 de agosto de 2020. Disponible en: <https://www.who.int/es/news-room/detail/29-06-2020-covidtimeline>.

ORIS (2020a). La Guardia Civil colabora en el reparto de medicamentos a los ciudadanos más alejados de los núcleos urbanos. Gabinete de Prensa. Web Oficial de la Guardia Civil. 21 de junio de 2020. Extraído el 1 de agosto de 2020 de: <https://www.guardiacivil.es/es/prensa/noticias/7310.html>

ORIS (2020b). La Guardia Civil ha realizado casi 50.000 servicios humanitarios durante el estado de Alarma. Gabinete de Prensa. Web Oficial de la Guardia Civil. 21 de junio de 2020. Extraído el 1 de agosto de 2020 de: <https://www.guardiacivil.es/es/prensa/noticias/7489.html>

Ortiz Chaparro, F. (1999). Los jóvenes en el teletrabajo. *Estudios de Juventud* número 46/1999. Extraído el 1 de agosto de 2020. Disponible en: <http://www.injuve.es/sites/default/files/Revista46-2.pdf>

Sánchez-Urán Azaña, Y. (2019). Adaptación de la jornada laboral y derecho de conciliación de la vida laboral y familiar. Factores de valoración en la ponderación judicial. *Revista de Jurisprudencia Laboral*, número 8/2019.

Fecha de recepción: 08/10/2020. Fecha de aceptación: 25/11/2020