El ciberataque sufrido por una la empresa puede justificar un ERTE por causa de fuerza mayor

Declara la Sala que el ataque de ciberseguridad sufrido por una empresa, cuya prestación se desarrolla mediante el uso de sistemas informáticos ha de ser calificado de fuerza mayor y, por tanto, se ha de autorizar el ERTE solicitado, pues el hecho de que sea previsible un ataque de ese tipo en una entidad cuyos medios materiales son esencialmente digitales, no lo convierte en evitable.

Señala que la empresa puede haber previsto en su actividad ordinaria la existencia de un ciberataque, pero hay algunos sucesos de este tipo que rebasan los tenidos en cuenta en el desenvolvimiento ordinario y, por ello, no pueden ser evitados. Así, si se trata de un suceso inevitable, que rebasa los que pueden ser tenidos en cuenta en el curso normal de la vida de la empresa, se estará ante un supuesto de fuerza mayor. Concluye el Tribunal que la concurrencia de fuerza mayor habilita a la empresa a la adopción de las medidas suspensivas reconocidas en el art. 47 del ET respecto de los trabajadores afectados.

TRIBUNAL SUPREMO

Sala de lo Social

Sentencia 908/2024, de 11 de junio de 2024

RECURSO DE CASACIÓN Núm: 144/2022

Ponente Excmo. Sr. MARIA LUZ GARCIA PAREDES

En Madrid, a 11 de junio de 2024.

Esta Sala ha visto el recurso de casación interpuesto por el Abogado del Estado, en la representación que tiene de la Administración General del Estado (Ministerio de Trabajo y Economía Social), al que se adhirió íntegramente la Confederación General del Trabajo (CGT) y en su nombre y representación don José María Trillo-Figueroa Calvo contra la Sentencia núm. 37/2022 de la Sala de lo Social de la Audiencia Nacional de 14 de marzo de 2022 en el procedimiento n.º 13/202, sobre impugnación de actos administrativos en materia laboral y de seguridad social a instancia de Ilunion Contact Center S.A.U. y en su nombre y representación D. Juan José Jiménez Remedios contra el Ministerio de Trabajo y Economía Social.

Se ha personado como parte recurrida, D. Juan José Jiménez Remedios, Letrado del Ilustre Colegio de Abogados de Sevilla, en nombre y representación de Ilunion Contact Center S.A.U.

Ha sido ponente la Excma. Sra. D.ª María Luz García Paredes.

ANTECEDENTES DE HECHO

PRIMERO. - El 14 de enero de 2022, D. Juan José Jiménez Remedios, Letrado del Ilustre Colegio de Abogados de Sevilla, actuando en nombre y representación de Ilunion Contact Center, S.A.U., presentó demanda contra el Ministerio de Trabajo y Economía Social, sobre impugnación de actos administrativos en materia laboral y de seguridad social, frente a la desestimación por silencio administrativo, del recurso de alzada interpuesto por la citada empresa frente a la Resolución dictada

por la Sra. Directora General de Trabajo D.ª Florinda, de fecha 15 de julio de 2021, por la que se denegaba la constatación de fuerza mayor en que se fundaba el Expediente de Regulación Temporal de Empleo (ERTE). De dicha demanda conoció la Sala de lo Social de la Audiencia Nacional, en la que tras exponer los hechos y motivos que estimó de aplicación terminó suplicando se dictara sentencia por la que se declare: "no conforme a derecho el acto impugnado y su anulación total y proceda a reconocer y constatar expresamente la concurrencia de fuerza mayor habilitando a la empresa a la adopción de las medidas suspensivas reconocidas en el artículo 47 del Estatuto de los Trabajadores respecto de los trabajadores afectados, (i) por la concurrencia de la nulidad del procedimiento y de la Resolución impugnada en base a los argumentos contenidos la presente demanda y/o (ii) subsidiariamente por los motivos de fondo expuestos".

SEGUNDO. - Admitida a trámite la demanda se celebró el acto del juicio, con la intervención de las partes y el resultado que se refleja en el acta que obra unida a las actuaciones. Recibido el pleito a prueba se practicaron las propuestas por las partes y declaradas pertinentes.

TERCERO.- En fecha 14 de marzo de 2022, se dictó sentencia por la Sala de lo Social de la Audiencia Nacional, en la que consta el siguiente fallo: "Estimamos la demanda formulada por D. JUAN JOSÉ JIMÉNEZ REMEDIOS, Letrado del Ilustre Colegio de Abogados de Sevilla, actuando en nombre y representación de ILUNION CONTACT CENTER, S.A.U., contra, el MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL, sobre, IMPUGNACIÓN DE ACTOS ADMINISTRATIVOS EN MATERIA LABORAL Y DE SEGURIDAD SOCIAL, declaramos la nulidad del acto impugnado, declaramos estimada por silencio administrativo la solicitud de declaración de fuerza mayor formulada por la empresa ILUNION CONTACT CENTER, S.A.U., como causa de la suspensión de relaciones laborales de los trabajadores afectados de su plantilla".

CUARTO. - En dicha sentencia se declararon probados los siguientes hechos:

"PRIMERO. - En fecha 21 de junio de 2021, se efectuó por la empresa demandante, ante la Dirección General de Empleo del Ministerio de Trabajo y Economía Social, solicitud de constatación de fuerza mayor, en que se fundaba expediente de regulación temporal de empleo que contemplaba medidas suspensivas y de reducción de jornada, que afectaban a un total de 1.192 trabajadores de la empresa, distribuidos en sus centros de trabajo de Madrid, Barcelona, Sevilla y Logroño.

SEGUNDO. - El 4 de julio de 2021, se recibió comunicación mediante correo electrónico, del registro electrónico Redsara, por el que se comunicaba que, la solicitud estaba siendo tramitada por la oficina de Registro General del Ministerio de Trabajo, Migraciones y Seguridad social.

TERCERO.- El 19 de julio de 2021, se recibió Resolución dictada por la Sra. Directora General de Trabajo D.ª Florinda, de fecha 15 de julio de 2021, por la que se denegaba la constatación de fuerza mayor en que se funda el Expediente de Regulación Temporal de Empleo (ERTE) solicitado por Ilunion Conctact Center, S.A.U. (en lo sucesivo, "ICC", la "Empresa" o la "Compañía"), confiriendo el plazo de un mes para formular recurso de alzada, de conformidad con lo previsto en los artículos 121 y 122 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas ("Ley 39/2015"). (Descriptor 3).

CUARTO. - El 13 de agosto de 2021 la parte actora presentó Recurso de Alzada frente a la antedicha Resolución denegatoria; todo ello, al amparo de lo dispuesto en los artículos 112, 121 y 122 de la Ley 39/2015. (Descriptor 4).

QUINTO. - I. Ilunion Contact Center, S.A.U., es una sociedad perteneciente al Grupo Ilunion - participado íntegramente por la Fundación ONCE dedicada desde sus inicios a la actividad del Contact Center o Telemarketing, consistente en el servicio de atención de llamadas telefónicas, mediante su emisión o su recepción, con la gestión de la información o las incidencias que dicha llamada genera. Forma parte intrínseca de su objeto social la promoción laboral de trabajadores discapacitados

mediante la realización de todas aquellas acciones de marketing a través del teléfono como son promociones, ventas, sondeos, encuestas y estudios de mercado. II. La empresa cuenta con 5 centros de trabajo distribuidos por la geografía nacional, enclavados en las provincias de Madrid, Sevilla, Barcelona; Jaén y La Rioja. III. Dentro de la tipología de servicios del sector de Contact Center, la actividad principal de la empresa se corresponde con los servicios de Atención al Cliente, que representan el 48% del sector. Esta tipología de Servicios sitúa a Ilunion como un proveedor eminentemente de atención. Entre los sectores a los que pertenecen los clientes de la Sociedad hemos de destacar los siguientes: - Clientes sector privado: o Sector Seguros: Segurcaixa Adeslas, Sanitas. o Sector Transporte: Renfe/Enterprice Atesa o Sector Turismo: NH/ Hesperia/ Ilunion Hotels o Sector Industria: Zardoya Otis o Sector Juego: ONCE - Clientes administración pública: o La Rioja (Cita Previa Sanitaria). o EPES (Salud Responde), o Consorcio Transporte Publico Andalucía. o CAM (Campaña 012). Cada sector requiere una solución determinada para cada tipología de campaña ejecutada por la empresa. Asimismo, cada cliente y la campaña de cada cliente requieren soluciones diferentes, específicas y personalizadas para cada servicio. Por motivos de eficiencia, la distribución de la plantilla del colectivo de operadores se organice por campañas y la especialización de los empleados en cada una de ellas; de tal forma que, cuanto mayor sea la demanda de llamadas de una campaña, habrá que destinar a un mayor número de operadores a la misma. Además, no sólo las funciones de los empleados son diferentes dependiendo del sector o cliente para el que desarrolle sus tareas de campaña, sino que, cada sector se comporta de manera diferente, con patrones de oferta y demanda diferentes, y con amenazas y oportunidades de mercado diferentes, de modo que, la adscripción de los empleados a campañas concretas favorece su especialización y permite la prestación de servicios de mayor eficiencia a los clientes de la empresa. IV. Para poder desarrollar dichas actividades, Ilunion Contact Center cuenta en la actualidad con dos áreas diferenciadas: personal de Estructura y personal de Operaciones. El personal de Estructura se subdivide en 6 áreas: (i) el personal dedicado a labores de apoyo técnico de sistemas de información, (ii) personal comercial (iii) departamento financiero (iv) área de Recursos humanos y relaciones laborales (v) personal encargado de tareas relacionadas con servicios generales y (vi) unidad de apoyo. Por su parte en el área de Operaciones se encuadran las diferentes ubicaciones físicas donde se prestan los servicios propios de la actividad de la Sociedad y que se encuentran ubicados en los centros de trabajo previamente señalados. Este colectivo de "Operaciones" es el encargado de llevar a cabo las actividades y funciones que engloban los servicios de telemarketing y Contact Center de Ilunion Contact Center. V. La Compañía emplea a un total de 2.158 personas trabajadoras, de las que afectadas por las medidas suspensivas y de reducción de jornada que se propusieron, únicamente estarían 1.192 dada cuenta de que éste fue el número de empleados que vieron imposibilitado el desarrollo de su actividad laboral. VI. Ilunion Contact Center, S.A.U pertenece junto con las sociedades Ilunion CEE Contact Center, S.A.U. y FITEX Ilunion, S.A. a la división del Grupo Ilunion, denominada ILUNION CONTACT CENTER BPO, división que tiene como actividad los servicios de centro de atención de llamadas y de gestión documental. VII. Las tres sociedades que conforman ILUNION CONTACT CENTER BPO cuentan con una infraestructura común, que se asienta principalmente en Madrid, aunque también existen sistemas específicos en el resto de las sedes de las mencionadas mercantiles. Es en la sede de Madrid situada en la Calle Julián Camarillo donde se encuentra el Centro de Procesamiento de Datos (en adelante "CPD"), que contiene los servidores donde están instalados los sistemas por donde fluye y se procesa la información digital necesaria para la prestación de los servicios, así como procesos administrativos internos y las infraestructuras de comunicaciones asociadas. Igualmente se encuentra el equipo físico de la centralita de llamadas, que es la infraestructura principal utilizada en los servicios, dado que gestiona todas las conversaciones telefónicas, el principal medio para el contacto que tienen los clientes finales con los servicios prestados. Por todo lo anterior, la actividad de los trabajadores de las tres sociedades depende de forma esencial del correcto funcionamiento de la mencionada infraestructura tecnológica y del CPD. Y ello, por cuanto necesitan para desarrollar su actividad de una computadora profesional

con sistema operativo Windows. VIII. El día 4 de junio de 2021 a las 5:15 a.m. se recibe en Ilunion Contact Center una incidencia alertando de que los Virtual Desktop Infrastructure (tecnología de virtualización de escritorio que almacena un sistema operativo en un servidor centralizado de un centro de datos) no funcionaban correctamente. Detectada la mencionada incidencia se contacta con la compañía que da soporte a las tres sociedades que conforman la unidad Ilunion Contact Center BPO, la empresa externa Unified Cloud Services (en adelante "UCS"), para identificar el problema y aplicar una solución. En ese periodo de tiempo se detecta que un servicio de Base de Datos tampoco funciona correctamente. IX. A las 6:02 a.m. UCS informa de que se está generando tráfico de datos hacia ellos y que sospecha que se trata de un virus ransomware. A las 6:40 a.m. se apaga el CPD completo y se procede a cortar las comunicaciones con todas las sedes de la división Contact Center BPO para evitar la distribución del virus. X. Inmediatamente, se informa del incidente a Grupo Ilunion, el cual convoca al Grupo de Respuesta ante Incidentes de Ilunion (GRI), formado diferentes proveedores externos de servicios y sistemas afectados por el incidente entre otros: CIOs del Grupo Ilunion y de la unidad de Contact Center, Responsable de Seguridad de los Sistemas de Información, Departamento Jurídico, Responsable de Infraestructura y Comunicaciones, y los equipos de soporte externo de Seguridad de la empresa UST-Global y de la consultora independiente Deloitte, decidiendo activar el incidente en la póliza de ciberseguridad del Grupo. En el seno de dicho Grupo de Respuesta se definen las líneas de trabajo principales asociadas al plan de acción para asegurar la contención, erradicación y recuperación del entorno afectado con la mayor agilidad y garantías posible; repartiéndose asimismo las tareas entre los distintos equipos involucrados. A las 08:53 a.m. Deloitte -experto independiente- procede a la activación del equipo de Respuesta a Ciberemergencias (Cyber Emergency Managment) e inicia el análisis forense comenzando por un equipo aislado de la red que se identifica como infectado. Se buscan en dicho portátil artefactos infectados por el malware y se identifican los siguientes: ASWA_Install_Log_000.log.RYK DumpStack.log.tmp.RYK Clasificación: Interna Icr.txt.RYK MSCCHRT20.OCX.RYK RyukReadMe.html Se concluye por la extensión de los archivos que se trata del ransomware RYUK. Las labores de investigación y comprobación realizadas por dicha empresa independiente -en estrecha colaboración con la Empresa y el resto de las sociedades de la unidad afectada, así como los 8 proveedores externos de servicios de estas- se han prologado por más de veinte días. XII. El 4 de junio de 2021, se informa de la brecha de seguridad sufrida a la Agencia Española de Protección de Datos (en lo sucesivo, "AEPD"), conforme a lo dispuesto en el artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. El día 6 de junio de 2021 se actualiza dicha información. XIII. El mismo día en el que se detecta el incidente, esto es, el 4 de junio de 2021, se remite comunicación a todos los clientes informándoles de: La existencia de un posible incidente de ciberseguridad. Las medidas preventivas adoptadas por la Empresa para evitar posibles fugas de información, así como otro tipo de consecuencias. Entre las medidas principales, destaca la desconexión del Centro de Procesamiento de Datos. De la activación de todos los protocolos correspondientes. Del grado de afectación de dichos hechos a los servicios prestados por la Empresa. Los días posteriores al incidente (5, 6, 7 y 8 de junio), se remiten nuevas comunicaciones a los clientes de la división, actualizando la información disponible sobre el incidente y los avances de la investigación: Las nuevas medidas preventivas adoptadas. La tipología del virus y todos los datos obtenidos de la investigación forense. El grado de afectación a los servicios prestados. XIV. Se informa inmediatamente a los trabajadores y a su representación unitaria de la imposibilidad de prestar servicios en las unidades afectadas, por la inutilización de las computadoras, impresoras, escáner, etc. así como consecuencia del riesgo existente en materia de seguridad de la información de no adoptarse las mencionadas medidas y la cesión de la actividad en las unidades afectadas. XV. Asimismo, una vez detectada la incidencia, desde la Dirección General se alerta de la incidencia informática a la Dirección de Contact Center BPO, así como del apagado del CPD, con la finalidad de que dichos responsables trasladen la información a los equipos de trabajo. De esta forma, se va informando de la incidencia a todos los equipos afectados, instándoles a cesar en la

prestación de servicios como medida adoptada por el GRI - esto es, no solo por la Empresa y Grupo Ilunion, sino siguiendo las recomendaciones de las empresas independientes UCS y Deloitte-. Asimismo, se convoca a la representación unitaria de los trabajadores para abordar con inmediatez la situación y valorar las distintas opciones a adoptar. XVI. El equipo de Forensic de la empresa externa Deloitte, pese a haber efectuado informe definitivo tras una investigación de más de veinte días la cual comenzó en el mismo momento en el que se detectó la presencia del virus -que en el momento de realización de la solicitud de constatación de fuerza mayor no era de carácter definitivo- no ha podido evidenciar el vector de entrada del ransomware. De esta forma, si bien se afirma en el antedicho informe que toda la actividad maliciosa se llevó a cabo por dos usuarios del dominio de la organización, se indica que no se ha podido evidenciar como se han podido comprometer las credenciales de dichos usuarios. Del informe definitivo, que constata las conclusiones alcanzadas ya de forma preliminar, de fecha 14 de julio de 2021 (documento n.º 2 de los acompañados al Recurso de Alzada), que elabora la empresa externa Deloitte, se colige lo siguiente: La infección viene motivada por un ransomware de la familia Ryuk. Se descarta una posible vulnerabilidad del sistema de seguridad perimetral de la organización como posible vector de entrada del virus. Las medidas adoptadas proactivamente por parte de la división ILUNION CONTACT CENTER BPO para la contención y recuperación del entorno afectado por el incidente han sido adecuadas, llevándose a cabo de forma ágil y mitigando por lo tanto considerablemente el riesgo de potenciales impactos adicionales o reincidencia a corto plazo. Cabe señalar las medidas a las que se refiere el mencionado informe y que fueron adoptadas con la finalidad de contener el impacto del incidente: o Apagado completo del CPD de la organización, con el fin de frenar la propagación del ransomware mientras se desarrolla la investigación forense del escenario identificado. De este modo, no existe tráfico saliente desde la organización a otros posibles servicios, ya que la red se encuentra completamente aislada. o Estudio de la implantación de un EDR, para la detección temprana de posibles piezas de malware que puedan registrarse en los equipos, así como la detección de los IOCs asociados a las piezas de malware extraídas propiamente del escenario acontecido y referentes al ransomware Ryuk y otros módulos de malware comúnmente empleados durante las fases de escalada de privilegios, movimientos laterales y comunicación contra servidores C&C de la cadena de ataque. o Deshabilitación de todas las unidades mapeadas y carpetas compartidas en red. o Revisión de creación o modificación ilegítima de nuevos usuarios a nivel de Active Directory. Asimismo, no se detectan o refieren brechas o fallos en la adopción de medidas preventivas por la Empresa. Prueba evidente, no solo de la rigidez del sistema de seguridad existente en la Empresa, sino también de la efectividad de las medidas adoptadas por la Empresa es que, pese a la actividad ilegítima sufrida en los servidores, según se desprende del informe la exfiltración de información de la organización se considera muy baja. XVII. El incidente se ha producido, pese a las políticas de seguridad de la información existentes en todas las empresas pertenecientes a la división ILUNION CONTACT CENTER BPO, entre las que cabe destacar las siguiente: Existencia de un Sistema de Gestión de Seguridad de la Información (SGCI) basado en la necesidad de que la Información esté en continua evolución y que dicha evolución en la madurez esté documentada y pueda ser verificada. Sistema que es revisado anualmente. El modelo en el que se basa el SGSI de ILUNION Contact Center BPO es el denominado Modelo PDCA (Planificar, Hacer, Revisar, Actuar, por sus siglas en inglés) con lo que anualmente, se hace una revisión de las medidas de seguridad que están implantadas y se promueve una mejora continua, basados en un análisis de riesgos. Certificación ISO/IEC 27001 de técnicas de seguridad de la información otorgada por AENOR y renovada anualmente por auditorías. Certificación ISO/IEC 27002 que desarrolla controles específicos distribuidos en 13 capítulos, que suman 133 controles. A nivel organizativo, la Empresa cuenta con un entramado de políticas, normas y procedimientos de seguridad que establecen las pautas para actuar de forma segura en torno a la información. Asimismo, la Empresa dispone de una Política de Seguridad (PO01) de la cual se derivan normas que cubren todos los capítulos que se desarrollan en la ISO 27002. Activos e información inventariados y controlados de forma periódica y clarificados según las

dimensiones de seguridad (Integridad, Disponibilidad y Confidencialidad). Control de acceso de tipo lógico a los sistemas en función de las necesidades del negocio y basados en el principio de mínimo privilegio. En lo referido a seguridad física de las instalaciones, se tienen establecidos controles de acceso y de seguridad ante amenazas externas y ambientales, así como seguridad interna para proteger los activos que en ellas se encuentren. Controles que regulan la seguridad en la operativa diaria sobre los sistemas de información, que comprenden la asignación nominativa de usuarios con exigencia de contraseñas complejas para su login; revisión periódica de los permisos y privilegios de los usuarios, con énfasis en aquellos usuarios administradores; segmentación de redes destinadas a servicios diferenciados; gestión de conexiones remotas seguras; programa antivirus actualizado en todos los equipos, gestionado de forma centralizada; realización periódica de copias de seguridad y almacenamiento en lugares seguros. El ciclo de desarrollo de software, así como de su adquisición a terceros, está fundamentado en protocolos robustos que exigen el desarrollo seguro, con garantías de actualización periódica y en los casos en que sea aplicable, auditorías específicas de hacking ético. Se tiene una plataforma de trabajo extendida a todos los miembros de la organización, para la gestión integral de incidentes, mediante la cual se mantiene un flujo de trabajo controlado y documentado de todos los eventos que pueden afectar la seguridad de la información en la empresa. Apoyo en empresas de soporte especializadas como Unified Cloud Services. Forensic con auditoría realizado por una empresa independiente, Deloitte. Antivirus Kaspersky en todos los portátiles y ordenadores de sobremesa, así como en los servidores de toda la división. Firewall para el control y autorización de tráfico e IDS de la empresa Fortinet en el perímetro de seguridad del Centro de Procesamiento de datos, que realizan un filtrado de las conexiones y análisis del caudal de tráfico de entrada y salida de Contact Center. XVIII. El ciber-incidente se ha sufrido en los sistemas ubicados en todas las sedes de las empresas que conforman la división ILUNION CONTACT CENTER BPO y en todos los ordenadores instalados (alrededor de 1.200 equipos diferentes). Consecuencia de que se han visto afectados todos los componentes que dependen de esta infraestructura, los trabajadores de las distintas sociedades se han visto imposibilitados para utilizar los programas computaciones para operar los servicios de Contact Center y gestión documental y, con ello, para prestar servicios. XIX. Consecuencia de lo anterior, con fecha 4 de junio de 2021, se suspendieron la mayor parte de los servicios que se prestaban a los clientes, quedando con ello sin actividad los empleados vinculados a dichas campañas, ante la imposibilidad de uso de las herramientas informáticas esenciales para el desarrollo de la actividad laboral. Y todo ello, por los riesgos anteriormente expuestos. Concretamente, se han visto afectadas por el ciberataque las 28 campañas desarrolladas para distintos clientes en los términos que se explicita en el apartado XIX de la demanda, que se da por reproducido. XX. Es preciso señalar que el restablecimiento pleno y seguro de los servidores y del sistema informático en su conjunto requiere de un proceso complejo y lento, el cual ha sido desarrollado en el Informe Técnico, que se acompañó a la solicitud de expediente suspensivo como documento n.º 6 y que, en todo caso, justifica que la duración de la medida de ERTE que se proponía por la Compañía. El ransomware es un programa de software malicioso que puede infectar un equipo o una red, cifrando la información, y que, con carácter general, muestra o genera mensajes que exigen el pago de una suma dineraria en criptodivisas para restablecer el funcionamiento del sistema. Los métodos de entrada de este malware son variados: mediante un enlace malicioso en una página web o la infección de un fichero compartido, siendo el más habitual el phishing. Es por esto por lo que, además del control de navegación para evitar sitios sospechosos de ocultar malware, de la continua actualización de los sistemas, de la protección de los mismos y de las medidas preventivas de backup - todas ellas implementadas en la forma explicitada con anterioridad por la empresa demandante- es imposible mantener una protección total ante una incidencia de este tipo (Memoria explicativa de las causas e informe técnico que se acompañaban a la misma como documentos 5 y 6, que obran en el expediente administrativo y descriptores 28 y 29, que se dan por íntegramente reproducidos).

SEXTO. -El número y clasificación profesional de trabajadores afectados por la medida, especificados por centro de trabajo, provincia y comunidad autónoma, es el relacionado en la descripción 27, cuyo contenido, se da por reproducido. Se da por reproducida la relación de trabajadores afectados por el ataque informático donde se refleja la recuperación paulatina de la actividad de la Empresa en el período comprendido entre el 4 de junio y el 24 de julio de 2021. (descripción 81).

SÉPTIMO. -Se dan por reproducidos los documentos relativos a la política de seguridad de la información de la empresa. (Descripción 32). Descripción de la arquitectura general de la red corporativa de ILUNION CONTACT CENTER BPO. (descripción 34). El Mapa de la red ILUNION CONTACT CENTER BPO. (descripción 35). Contrato de prestación de servicios VID entre la demandante y Unified Cloud Services de 1 de mayo de 2020. (descripción 36). El procedimiento de gestión de Incidencias de Seguridad Informática. (descripción 37). El Manual de respuesta técnica frente a Ransomware. (descripción 38). La Póliza de Responsabilidad Civil por Riesgos Cibernéticos suscrita por Grupo Ilunion y sus filiales con la compañía de seguros AIG EUROPE, S.A. (descripción 39). Certificado de la compañía de seguros AIG EUROPE, S.A. relativo a la póliza del Grupo Ilunion y sus filiales para el periodo comprendido entre el 24 de abril de 2021 y el 24 de abril a las 2022. (descripción 40). El Manual en materia de seguridad de la información y ciberseguridad facilitado a la plantilla con ocasión de los cursillos de iniciación en la Empresa. Mediante distintos módulos se informa a los trabajadores de las pautas de prevención en el manejo en el día a día de los distintos dispositivos informáticos y aplicaciones puestas a su disposición. (descripción 78).

OCTAVO.-El 14 de julio de 2021, se emitió informe por la Inspección de Trabajo y Seguridad Social que concluye: "A criterio de la actuante, de conformidad con el art. 7.3 y 51.7 del Texto Refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, y en los artículos 31 y siguientes del Real Decreto 1483/2012 de 29 de octubre, por el que se aprueba el Reglamento de los procedimientos de despido colectivo, la solicitud formulada no puede encuadrarse en los supuestos de suspensión por fuerza mayor. En virtud de lo expuesto, se informa desfavorablemente a la fuerza mayor invocada del art. 47.3 del Estatuto de los Trabajadores. (descripción 4 del expediente administrativo).

NOVENO. -Se ha agotado la vía administrativa, habiéndose interpuesto recurso de alzada por la parte demandante en plazo, que ha sido desestimada por silencio administrativo al haber transcurrido el plazo de tres meses para su resolución sin que recaiga resolución expresa. (expediente administrativo).

DÉCIMO. -Consta en el expediente administrativo, informe del subdirector General de Relaciones Laborales que considera que las razones que aporta la empresa no resultan suficientes a los efectos de su calificación como determinante de una situación de fuerza mayor. La remisión a los posibles impedimentos previsibles en su actividad principal no muestra la vinculación directa con fuerza mayor establecida en el artículo 47 del Estatuto de los Trabajadores, sino que lleva a la conclusión de que se debieron reconducir a causas técnicas, organizativas o de producción".

QUINTO. - Contra dicha resolución se interpuso recurso de casación por el Abogado del Estado, en la representación que tiene de la Administración General del Estado (Ministerio de Trabajo y Economía Social), siendo admitido a trámite por Providencia de esta Sala de 12 de septiembre de 2022. Por escrito de D. José María Trillo-Figueroa Calvo, en nombre y representación de la Confederación General del Trabajo (CGT), se adhirió al recurso de la demandada.

SEXTO. - Impugnado el recurso por Ilunion Contatc Center S.A.U, se emitió informe por el Ministerio Fiscal en el sentido de considerar el recurso improcedente, e instruida la Excma. Sra. Magistrada Ponente se declararon conclusos los autos, señalándose para votación y fallo el día 11 de junio de 2024, fecha en que tuvo lugar

FUNDAMENTOS DE DERECHO

PRIMERO. - La Sala de lo Social de la Audiencia Nacional ha dictado sentencia el 14 de marzo de 2022, en el proceso de impugnación de actos administrativos de naturaleza laboral seguido bajo el número 13/2022, a instancia de la empresa Ilunion Contatc Center S.A.U, en la que estima la demanda considerando la existencia de silencio administrativo positivo en relación a la solicitud de declaración de fuerza mayor formulada por la empresa Ilunion Contact Center, S.A.U..

La cuestión suscitada en el presente procedimiento es, primero, la de determinar si la solicitud de autorización de ERTE por fuerza mayor presentada por la empresa demandante fue estimada por silencio positivo, al haber resuelto la Administración demandada más allá del plazo de 5 días legalmente establecida al efecto y, segundo, de entender que la Resolución no fue estimada por silencio positivo y, por tanto, fue desestimatoria, resolver si concurre causa de fuerza mayor.

Frente a dicha resolución judicial estimatoria de la demanda se ha interpuesto por el Abogado del Estado, en la representación que tiene de la Administración General del Estado (Ministerio de Trabajo y Economía Social), recurso de casación ordinaria amparado en un motivo único de recurso, por infracción de las normas del ordenamiento jurídico relativas a la ampliación del plazo de resolución en el procedimiento administrativo de los ERE, con sede en el art. 207 e) de la LRJS; en concreto alega la infracción de los arts. 32.4 y 47.1.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), en relación con las demás normas que cita y con la jurisprudencia.

La parte recurrida Ilunion Contact Center SAU impugnó el recurso y alegó que ningún hecho que podría excusar el incumplimiento de los plazos fijados para resolver por la Administración demandada figura en los Hechos Probados de la Sentencia y que, en todo caso, la sentencia recurrida ha apreciado que concurría la fuerza mayor, lo que no se combate por la recurrente en su recurso. Añade que, la Administración resolvió fuera de plazo, alegando una supuesta incidencia técnica que le habría impedido resolver en tiempo, pero no ha quedado acreditada la misma, antes al contrario, constan actuaciones de la demandada que evidencian que en el eventual caso de haber existido la incidencia que pretendidamente motivaría la ampliación del plazo, esta no impedía el desarrollo de actividad de la Administración, de modo que la fecha de la presunta reanudación de la actividad normal del Ministerio que se alega en su Resolución es arbitraria e interesada. Por otro lado, sostiene que se pretende también limitar la eficacia y fuerza jurídica del silencio administrativo con base en unos preceptos y una jurisprudencia, en ningún caso aplicable al caso objeto de autos. Cita la Sentencia de esta Sala de 25 de enero de 2021, sobre la interpretación de los preceptos que reglan los procedimientos de suspensión de contratos de trabajo por causa de fuerza mayor. Alega también la grave vulneración al principio de seguridad jurídica consagrado en el artículo 9.3 de la CE que supondría que la Administración quedara presuntamente legitimada para incumplir los plazos legales y para alterar, en cualquier momento, el sentido de una resolución estimatoria por silencio administrativo, cuando, además, la recurrente reconoce en la resolución impugnada la adecuación de la solicitud y el cumplimiento por parte de la actora de todas las formalidades. Por último, y sobre la concurrencia de fuerza mayor, insiste en que no se combate de contrario la estimación subsidiaria de la demanda con base en la concurrencia de la fuerza mayor, de modo que, de estimar el único motivo del recurso, ello no conduciría a la desestimación de la demanda como se solicita en el suplico del Recurso. Cita la sentencia de esta Sala de 8 de julio de 2008 (rec. 1857/2007) sobre la fuerza mayor en el marco de las relaciones laborales, concluyendo que se dan todas las notas que la conforman, ya que el análisis de los elementos configuradores de la fuerza mayor permite concluir que el ataque informático a través de un virus *ransomeware* que se tradujo en el "secuestro" de la información clave de la empresa, afectando de forma determinante a su operatividad, puede ser calificado como un supuesto de fuerza mayor en los términos de la doctrina citada de esta Sala y que, por tanto, la resolución denegatoria de la fuerza mayor que ha sido confirmada en alzada conculca de forma

palmaria lo preceptuado en los artículos 47 y 51.7 del ET. Que la imposibilidad objetiva que describe la fuerza mayor no queda circunscrita a fenómenos naturales, pudiéndose predicar (siempre que concurran los elementos configuradores) a fenómenos que tienen su origen en el comportamiento humano. En la medida que se vio afectado el Centro de Procesamiento de Datos (CPD), en la división Ilunion Contact Center BPO, se produjo la inutilización de servidores, sistemas electrónicos, computadoras (en número aproximado 1.200) e impresoras (afectando en un primer estadio, en la ejecución de 28 campañas - y a 1.192 empleados de la Empresa). Efectos impeditivos que no pueden quedar desvirtuados por la simple manifestación de que los trabajadores "quedaron en régimen de disponibilidad para la empresa", no siendo ello elemento suficiente para impedir la suspensión de sus contratos, pues las personas trabajadoras pueden manifestar estar disponibles para realizar actividad laboral, pero si no pueden realizarla porque no existen elementos con los que ejecutar su desarrollo, la disponibilidad se traduce en "hacer nada". Que, en este caso, no puede hablarse propiamente de una mera "avería" de los equipos imputable a la empresa. Añade que existe una estrecha (e indudable) relación causal entre el hecho obstativo (el ataque y el "secuestro" de datos) y la imposibilidad material de la empresa de dar ocupación de trabajo a las personas trabajadoras. Que basta la mera lectura de los informes técnicos y periciales obrantes en el expediente administrativo y que se dan por reproducidos en la sentencia sometida a debate casacional, para colegir como el bloqueo de los servicios se traduce en una imposibilidad manifiesta de prestación de servicios. Que el ataque no fue "causado" por la Empresa (y, en este sentido, puede afirmarse que es claramente inimputable), y la misma obró con la "diligencia normal" y, asimismo, ha articulado medidas preventivas dirigidas a reducir el riesgo, con instrumentos y protocolos preventivos y los ha puesto efectivamente (y de forma constante) en práctica para rebajar, en la medida de lo razonable (técnica y humanamente), el riesgo de un ciber ataque. Concluye que, si bien el ciberataque no es hecho, propiamente, "imprevisible", ello no impide que este tipo de sucesos, por el solo hecho de haber sido valorados, queden descartados automáticamente como susceptibles de generar una situación de excepción. Que la empresa ha adoptado medidas de protección reforzadas -en comparación con las adoptadas por empresas de fuera del sector- como certificados ISO otorgados por Aenor, pólizas de ciberseguridad, procedimientos y protocolos de actuación, entre otras muchas, lo que es una circunstancia que, no solo no aleja el ataque sufrido por la Empresa del ámbito de la fuerza mayor, sino que por el contrario es la que acredita lo inevitable del suceso. En suma, al ser un riesgo que entra dentro del "imaginario" de sucesos posibles y, por ende, que no puede catalogarse de "imprevisible", es la adopción de todas las medidas posibles -dentro de unos límites humanos y técnicos razonables- lo que hace que el riesgo devenga inevitable. Y es la existencia de esta alternativa -la inevitabilidad- en el caso de autos, la que produce la situación de excepción alegada, en la que ni siquiera se conoce qué medida concreta podría articularse para la evitación del incidente, dada cuenta de que se desconoce la vía de entrada del mismo. Cita a continuación las medidas que conforman la política de seguridad. Por todo ello, finalmente, señala que para el hipotético supuesto de que se estimara el motivo único del recurso, procedería la estimación de la demanda rectora de autos por los motivos constatados por el Tribunal *ad quo* en la Sentencia recurrida.

La CGT se adhirió al recurso del Ministerio demandado y, en primer término, manifiesta su adhesión respecto a la ampliación del plazo de resolución en el procedimiento administrativo, en el sentido del art. 32.4 de la Ley 39/2015, de 1 de octubre, del PACAP, en cuanto que se trató de un incidente técnico que afectó de manera pública y manifiesta al funcionamiento ordinario de la Administración y así se resolvió expresamente mediante resolución de 16 de junio de 2021. Que el hecho de que se pudiera registrar la solicitud del ERTE en modo alguno indica que el funcionamiento ordinario del Ministerio no se encontrase afectado. En segundo lugar, que no puede sostenerse que un ataque informático en una empresa digital como la demandante, cuya prestación se desarrolla en esencia dentro del uso de sistemas informáticos, software, aplicaciones, etc., pueda ser calificada de fuerza mayor, ya que, ante la situación del teletrabajo, la empresa mantuvo el mismo sistema de protección

que cuando se prestaba en plataforma. Es la única empresa del sector que ha visto afectada su prestación por un ataque informático y, en todo caso, la misma puede conllevar una razón técnica o productiva, pero no de Fuerza Mayor, precisamente por su previsibilidad y evitabilidad. Cita Sentencia de esta Sala de 8 de julio de 2008 y, más recientemente, la STS núm. 927/2021 de 22 septiembre, que aborda el concepto de fuerza mayor. En tal sentido, no se trata de un hecho imprevisible, la posibilidad de un ataque informático que sufren continuamente las empresas y, menos tratándose de una dedicada a la gestión de información sobre la utilización de sistemas tecnológicos e informáticos. Se trata de un riesgo eminentemente derivado de la propia realidad productiva. Este incidente se hubiese evitado con la existencia de copia de seguridad (Back Up) con otro CPD, tal y como utilizan otras empresas del sector y que en todo caso debería considerarse dentro de la esfera de riesgos asumidos por el empresario dado el carácter de su actividad y, por ello, en todo caso susceptible de suspensiones derivadas de causas ETOP. Cita el ámbito funcional de II Convenio colectivo de ámbito estatal del sector de Contact Center (antes telemarketing). Finalmente, señala que los trabajadores siguieron prestando su actividad mediante su puesta a disposición del empleador durante toda su jornada. Así se recoge en el propio Hecho Probado Sexto de la sentencia y así se acreditó en el expediente administrativo por las representaciones de los trabajadores CCOO, UGT y CGT y el propio informe de la ITSS.

Se emitió informe por el Ministerio Fiscal en el sentido de considerar que el recurso debe ser desestimado, pues las alegaciones de la parte recurrente no pueden prosperar, toda vez que en ningún momento se acredita que la demandada sufriera una incidencia técnica que imposibilitara el funcionamiento ordinario de trabajo de ese Organismo. Y si ello hubiera acaecido, el Ministerio tiene los medios técnico-materiales suficientes para hacer llegar su comunicación al interesado a través de otros canales, incluso podría suspender el plazo de contestación, lo que no ocurrió, ya que, si bien existió una Resolución en tal sentido, de 16 de junio de 2021, no fue hasta un mes después cuando se dio contestación por parte de la Dirección General. Que la resolución obtenida a través del silencio positivo no es *contra legem* en virtud del art. 47 de la LPAC, sino que la misma cumple los requisitos exigidos y los plazos adecuados. Asimismo, el Ministerio Fiscal sostiene que queda acreditada también la existencia de una fuerza mayor sobrevenida.

SEGUNDO. - 1. En su primer y único motivo de recurso, la Administración recurrente, al amparo del art. 207.e) de la LEJS, alega la infracción de las normas del ordenamiento jurídico aplicables para resolver las cuestiones objeto de debate, en concreto, los arts. 32.4 y 47.1.f) de la LPACAP, en relación con las demás normas que son luego citadas y con la jurisprudencia. Alega que la sentencia recurrida ha mezclado dos elementos del art. 32.4 de la LPACAP que, sin embargo, son del todo diferentes, a saber, por un lado, la concurrencia de la causa habilitante para la ampliación del plazo de resolución, y, por otro, la duración misma de dicha ampliación, ya que para que quepa ampliar los plazos es necesario un doble requisito, a saber (i) que concurra una incidencia técnica, cualquiera que sea ésta, informática o no, ya que la ley no distingue; y (ii) que esa incidencia técnica haya imposibilitado el funcionamiento ordinario del sistema, sin que la Ley distinga tampoco cuál sea el origen, previsible o no, y evitable o no, de la incidencia. Ahora bien, una vez que los plazos se han ampliado por concurrir el presupuesto habilitante (la incidencia técnica que imposibilita el funcionamiento ordinario), la duración misma de la ampliación es indefinida, puesto que alcanza hasta que se solucione el problema, es decir, hasta que la Administración pueda restablecer el estándar ordinario o habitual de su actividad. Que, el Ministerio de Trabajo y Economía Social sufrió un ciberataque que afectó gravemente a sus servicios y que imposibilitó su funcionamiento ordinario, de modo que hubo de dictar una Resolución *ad hoc*, de fecha 16 de junio de 2021, para ampliar los plazos administrativos, al amparo del art. 32.4 de la LPACAP, ya que la incidencia técnica sufrida imposibilitaba el funcionamiento ordinario del sistema, sin que el mero hecho de que el Registro General del Ministerio pudiera funcionar de forma aislada (como, por ejemplo, el 3 de julio, al que se refiere la Sentencia recurrida), convierta a ese hecho aislado en una regla general de funcionamiento ordinario de todos

los servicios. Así, pues, la Resolución ampliatoria de 16 de junio de 2021 (no impugnada, ni impugnable, en este proceso ante el orden social), determinó con total licitud que la ampliación de los plazos no vencidos alcanzara hasta que se solucionase el problema. Por consiguiente, no cabe en modo alguno entender que la Administración dictó su resolución fuera de plazo y que, por ende, la empresa haya visto estimada por silencio positivo su solicitud de ERE por fuerza mayor. En segundo lugar, aun admitiendo, a efectos meramente dialécticos, que tal hubiera sucedido, lo que está igualmente claro es que en ningún caso cabe adquirir por silencio positivo unas facultades que sean contrarias al ordenamiento jurídico, como ha resuelto la Sentencia recurrida. La Administración dictó de forma expresa la antedicha Resolución de 15 de julio de 2021 por entender no sólo que estaba dentro del plazo legal para hacerlo, sino, sobre todo, porque la solicitud de la empresa actora no podía ser admitida, porque implicaba obtener por silencio positivo unas facultades que eran contrarias al ordenamiento jurídico. Dicho de otra manera, la Administración rechazó de forma expresa la solicitud de ERE por fuerza mayor porque así lo establece la doctrina jurisprudencial para aquellos casos en los que se ha obtenido por silencio positivo una prestación *contra legem*. Alude al art. 47.1.f) de la LPACAP que establece que son nulos de pleno derecho "f) Los actos expresos o presuntos contrarios al ordenamiento jurídico por los que se adquieren facultades o derechos cuando se carezca de los requisitos esenciales para su adquisición". Cita STS, Sala Tercera, núm. 1769/2018, de 13 de diciembre de 2018 (rec. 568/2017); doctrina que rige también en el ámbito ius laboral estricto. Cita a tal efecto, la STS 623/2017, de 13 de julio de 2017 (recurso 2976/2015), que estableció que no son válidas las condiciones más beneficiosas *contra legem.* A continuación, sostiene que la concreta situación padecida por la empresa no puede considerarse en modo alguno como un caso de fuerza mayor, en virtud del cual la empresa reciba un beneficio económico con cargo a los fondos públicos por algo que ni era imprevisible ni era tampoco inevitable para una empresa de la actividad de la que aquí se trata, dedicada a la actividad del Contact Center o Telemarketing, consistente en el servicio de atención de llamadas telefónicas, mediante su emisión o su recepción, con la gestión de la información o las incidencias que dicha llamada genera y que, sobre todo, no dio lugar a que se dejara de trabajar o a que el trabajo quedara imposibilitado. Añade que no se trata tanto de que existiera una causa ajena a la voluntad empresarial, sino de que, en definitiva, ello no dio lugar a que la prestación personal del trabajo no pudiera llevarse a cabo, lo que impide que pueda calificarse como fuerza mayor. La fuerza mayor implica la imposibilidad de trabajar, aspecto que no ha quedado acreditado en los HH.PP., a la luz de las declaraciones de los trabajadores y la justificación documental aportada, ya que la actividad ordinaria de la empresa se vio parcialmente afectada, pero los trabajadores estuvieron en todo momento a disposición de la empresa, ya sea presencialmente o teletrabajando, e informaron a la empresa sobre sus descansos, comienzo y final de la jornada, así como de citas médicas para poder ausentarse de su puesto de trabajo, todo según consta en el expediente y en los HH.PP. (vid. el HP 6.º y la documentación remitida en él). Concluye, pues, negando la validez jurídica de la conducta de la empresa, ya que no existía una causa de fuerza mayor impeditiva.

2. - La Sentencia impugnada por su parte considera que desde que se efectúa la solicitud de ERTE por causa de fuerza mayor (21 de junio de 2021), hasta que se dicta resolución (15 de julio de 2021), transcurren un total de 18 días hábiles, lo que excede con creces el plazo máximo de 5 días hábiles que para dictar resolución establece el art. 33 del Real Decreto 1483/2012, de 29 de octubre, por el que se aprueba el Reglamento de los procedimientos de despido colectivo y otros; y que la falta de respuesta expresa dentro del plazo legal determina que la solicitud se entienda estimada por silencio positivo, sin que la Administración pueda dictar una resolución expresa posterior, salvo para confirmar el acto y que, aunque el plazo estaba ampliado por aplicación del art. 34.2 de la LPACAP, no es menos cierto que el mismo exige que la citada incidencia haya imposibilitado el funcionamiento ordinario del sistema o aplicación que corresponda y, en este caso, existen actuaciones dentro del expediente anteriores a la citada fecha de 8 de julio de 2021 que revelan que, en el eventual caso de haber

existido la incidencia que pretendidamente motiva la ampliación del plazo, ésta no impedía el desarrollo de actividad de la Administración.

3.- A los procedimientos del RD 1482/2012 les es de aplicación supletoria la LPACAP, de manera que el plazo de emisión de la resolución sobre la solicitud de ERE del art. 33 del RD 1482/2012 se debe insertar dentro del régimen jurídico general de los procedimientos administrativos y, en concreto, de los preceptos que regulan la ampliación de los plazos procedimentales en la LPACAP.

A tal efecto, el art. 33 del RD 1482/2012 relativo a Instrucción y resolución de la extinción y suspensión de relaciones de trabajo y reducción de jornada por fuerza mayor establece que: "1. La autoridad laboral competente recabará, con carácter preceptivo, informe de la Inspección de Trabajo y Seguridad Social, y podrá realizar o solicitar cuantas otras actuaciones o informes considere indispensables.

No obstante lo anterior, la solicitud del informe de la Inspección de Trabajo y Seguridad Social no será preceptiva en los casos en que la fuerza mayor temporal venga determinada por los impedimentos o limitaciones en la actividad normalizada de la empresa a los que se refiere el artículo 47.6 del Texto refundido de la Ley del Estatuto de los Trabajadores.

2. La autoridad laboral dictará resolución en el plazo máximo de cinco días a contar desde la fecha de entrada de la solicitud en el registro del órgano competente para su tramitación".

El art. 22 de la LPACAP dispone: "El transcurso del plazo máximo legal para resolver el procedimiento y notificar la resolución se podrá suspender en determinados supuestos (...) d) Cuando se soliciten informes preceptivos a un órgano de la misma o distinta Administración, por el tiempo que medie entre la petición, que deberá comunicarse a los interesados, y la recepción del informe, que igualmente deberá ser comunicada a los mismos. Este plazo de suspensión no podrá exceder en ningún caso de tres meses. En caso de no recibirse el informe en el plazo indicado, proseguirá el procedimiento".

El art. 23 de la LPACAP: "1. Excepcionalmente, cuando se hayan agotado los medios personales y materiales disponibles a los que se refiere el apartado 5 del artículo 21, el órgano competente para resolver, a propuesta, en su caso, del órgano instructor o el superior jerárquico del órgano competente para resolver, podrá acordar de manera motivada la ampliación del plazo máximo de resolución y notificación, no pudiendo ser este superior al establecido para la tramitación del procedimiento.

2. Contra el acuerdo que resuelva sobre la ampliación de plazos, que deberá ser notificado a los interesados, no cabrá recurso alguno".

El art. 32.1 de la LPACAP establece que: "La Administración, salvo precepto en contrario, podrá conceder de oficio o a petición de los interesados, una ampliación de los plazos establecidos, que no exceda de la mitad de los mismos, si las circunstancias lo aconsejan y con ello no se perjudican derechos de tercero. El acuerdo de ampliación deberá ser notificado a los interesados".

El art. 32.4 de la LPACAP dispone que: "Cuando una incidencia técnica haya imposibilitado el funcionamiento ordinario del sistema o aplicación que corresponda, y hasta que se solucione el problema, la Administración podrá determinar una ampliación de los plazos no vencidos, debiendo publicar en la sede electrónica tanto la incidencia técnica acontecida como la ampliación concreta del plazo no vencido".

De este modo, el plazo máximo legal para resolver el procedimiento (5 días) y notificar la resolución (10 días) se puede suspender o ampliar en los términos previstos en los arts. 22 y 23 de la LPACAP, respectivamente. El art. 32.4 de la misma norma, por su parte, regula la ampliación de los plazos en el supuesto de una incidencia técnica.

4.- En este caso, el plazo de cinco días para resolver podría haberse suspendido conforme permite el art. 22 de la LPACAP por razón de la petición de Informe a la ITSS, al tratarse de una Informe preceptivo, según dispone el art. 33.1 del RD 1482/2012. Además, la sentencia recurrida declara probado que el 9 de julio de 2021, la ITSS recibió requerimiento de documentación, citando a la Empresa a comparecencia en fecha 13 de julio de 2021. El Informe de la ITSS lleva fecha de 14 de julio de 2021. Dicha suspensión, sin embargo, exige una comunicación al interesado de que se ha pedido ese Informe preceptivo y, después, otra comunicación de que ese Informe se ha recibido. No constan acreditadas ninguna de ellas. De hecho, la propia Administración solo alude en su Resolución de 15 de julio de 2021, que por previa Resolución de 16 de junio de 2021 se produjo una ampliación del plazo para resolver, de modo que lo que procede analizar es, precisamente, si había razones para la ampliación y si esta se produjo conforme a derecho.

5.- La ampliación de los plazos regulada en el art. 32 de la LPACAP tiene un régimen jurídico distinto en función de si la misma deriva o no de un incidente técnico. En el art. 32.1 se regula la ampliación por circunstancias que lo aconsejen, lo que requiere la notificación a los interesados. Así, la STS, Sala Tercera, de lo Contencioso núm. 494/2023, de 19 de abril de 2023, alude al art. 32 de la Ley 39/2015 en el sentido de que la Administración puede conceder una ampliación de los plazos que no exceda de la mitad de los mismos y, añade que: "Sin embargo, del art. 32 de la Ley 39/2015 se infiere, primero, que la resolución administrativa será expresa (por cuanto deberá ser notificarse a los interesados) y segundo, que esa resolución será motivada pues habrá que tener en cuenta "si las circunstancias lo aconsejan y con ello no se perjudican derechos de tercero".

Pero, si la ampliación deriva de una incidencia técnica, el art. 32.4 solo exige la publicación en la sede electrónica, tanto de la incidencia técnica acontecida como de la ampliación concreta del plazo no vencido, ya que, en este caso, a tenor de lo dispuesto en la propia LPACAP, la ampliación perdura hasta que se resuelva el problema.

Si accedemos a la sede electrónica del Ministerio de Trabajo, comprobamos como consta la publicación de la incidencia y, también, la determinación de la ampliación concreta del plazo no vencido: desde el 16 de junio hasta el 8 de julio.

En efecto, por Resolución de 16 de junio de 2021, se produjo esa concreta ampliación para todos los procedimientos que se indican a continuación:

"I. Procedimientos previstos en el Real Decreto 1483/2012, de 29 de octubre, por el que se aprueba el Reglamento de los procedimientos de despido colectivo y de suspensión de contratos y reducción de jornada.

II. Procedimiento de depósito de estatutos previsto en el Real Decreto 416/2015, de 29 de mayo, sobre depósito de estatutos de las organizaciones sindicales y empresariales.

III. Procedimientos de autorización y extinción de empresas de trabajo temporal a los que se refieren la Ley 14/1994, de 1 de junio, por la que se regulan las empresas de trabajo temporal y el Real Decreto 417/2015, de 29 de mayo, por el que se aprueba el Reglamento de las empresas de trabajo temporal.

IV. Procedimiento para la imposición de sanciones por infracciones en el orden social competencia de esta Dirección General, de conformidad con lo referido en el Real Decreto 928/1998, de 14 de mayo, por el que se aprueba el Reglamento general sobre procedimientos para la imposición de sanciones por infracciones de orden social y para los expedientes liquidatorios de cuotas de la Seguridad Social".

También se recoge la determinación concreta de la ampliación en el sentido de que: "En su virtud, mediante esta comunicación se hace público que el número de días por los que se han de entender ampliados los plazos máximos de resolución y notificación de los procedimientos antes referidos que

son competencia de esta Dirección General, y durante los cuales no ha sido posible el uso de los sistemas y aplicaciones informáticas del Ministerio, es el siguiente:

-En el caso de procedimientos administrativos cuyos plazos estén expresados en días, la ampliación se entenderá realizada por tantos días hábiles como existan en el período comprendido entre el 16 de junio y el 8 de julio de 2021, ambos inclusive (en total, 17 días hábiles).

- En el caso de procedimientos administrativos cuyos plazos estén fijados en meses, la ampliación se entenderá realizada por el total de días naturales comprendidos entre el 16 de junio y el 8 de julio de 2021, ambos inclusive (en total, 23 días)"

Lo anterior coincide exactamente con el contenido de la Resolución impugnada de 15 de julio de 2021 (descriptor 3), cuando recoge que, a los efectos de "(...) los plazos máximos de resolución y notificación se hace constar que, con motivo del incidente de ciberseguridad sufrido a partir del día 9 de junio de 2021 por el Ministerio de Trabajo y Economía Social, la Dirección General de Trabajo dictó la Resolución de fecha 16 de junio de 2021 sobre ampliación de plazos en el ámbito de actuación y funcionamiento de la propia Dirección General mediante la que se amplían, hasta que se resuelvan las incidencias técnicas que imposibilitan el funcionamiento ordinario de los sistemas y aplicaciones informáticas del Ministerio de Trabajo y Economía Social, incluyendo su sede electrónica, los plazos máximos de resolución y notificación aplicables a, entre otros, los procedimientos previstos en el Reglamento aprobado por el Real Decreto 1483/2012, 29 de octubre, norma de aplicación a este expediente".

También se indica que: "dicha ampliación de plazos se entiende producida respecto del presente procedimiento (cuyo plazo de resolución está fijado en días) por tantos días hábiles como existen en el período comprendido entre el 16 de junio de 2021 (inicio de la ampliación) y el 8 de julio de 2021 (fin de la ampliación), ambos inclusive".

Si bien en los hechos probados no consta expresamente mencionada la Resolución de 16 de junio de 2021 por la que se amplían los plazos y se determina la concreta ampliación en relación a los procedimientos que allí se citan, no es en realidad un hecho controvertido. La empresa al impugnar el recurso se limita a alegar que no consta acreditada la incidencia técnica, pero lo cierto es que la Resolución de 16 de junio de 2021 no ha sido impugnada en este procedimiento. La sentencia recurrida alude a la misma y acepta incluso que la misma amplió el plazo para resolver, aunque después niega que la citada incidencia haya imposibilitado el funcionamiento ordinario del sistema, al existir actuaciones dentro del expediente que revelan que la misma no impidió el desarrollo ordinario de la actividad de la Administración (cita expresamente la existencia acreditada de actividad del Registro del Ministerio el día 3 de julio)

Los anteriores argumentos no pueden ser aceptados. En primer lugar, como decimos, la propia sentencia, con indudable valor fáctico, alude a la existencia de la Resolución de la demandada de fecha 16 de junio de 2021, publicada en su sede electrónica, conforme a la cual el plazo de 5 días fue ampliado por tantos días hábiles como existen en el período comprendido entre el 16 de junio de 2021 (inicio de la ampliación) y el 8 de julio de 2021 (fin de la ampliación), ambos inclusive, de modo que el plazo de cinco días para resolver del art. 33 del RD 1482/2012 se vio ampliado, computado el mismo desde el fin de la ampliación (8 de julio) hasta la fecha de la Resolución (15 de julio).

En segundo lugar, es público y notorio que esa misma incidencia técnica provocó, y así consta en la misma sede electrónica de la Seguridad Social, que tanto el INSS, como la TGSS, como la ITSS, emitieran Resoluciones similares (de ampliación de plazos para resolver). En estos tres casos, la ampliación de los plazos fue muy superior a la decretada por la Dirección General de Trabajo, ya que tanto el INSS, como la TGSS, como la ITSS, entendieron ampliados los plazos por el período de los días hábiles comprendidos entre el 16 de junio y el 31 de agosto 2021, ambos inclusive, en relación a

aquellos procedimientos administrativos competencia del INSS y de la TGSS que requerían de actuaciones de la ITSS (actuaciones de declaración de responsabilidad empresarial por falta de medidas de seguridad y salud en el trabajo; elevación a definitiva de las actas de liquidación de cuotas y de las actas de liquidación conjuntas con las actas de infracción; imposición de sanciones en materia de Seguridad Social, etc.), lo que denota que la incidencia técnica tuvo diferente repercusión dentro del mismo Ministerio de Trabajo, lo que puede explicar, por ejemplo, que el Registro General del Ministerio pudiera funcionar el día 3 de julio, como pone de manifiesto la Sentencia recurrida, como argumento para denegar el normal funcionamiento de dicha demandada.

En definitiva, la Resolución de 15 de julio de 2021 no es extemporánea, se dictó dentro de plazo y, por ello, no puede concluirse que el ERE por fuerza mayor fue autorizado por efecto del silencio positivo.

TERCERO. - 1. Estimado el motivo del recurso del Abogado del Estado destinado a combatir que la Resolución de la Dirección General de Trabajo de 15 de julio de 2021 se había dictado fuera de plazo, como resolvió la SAN recurrida, procede a continuación entrar en el fondo del asunto en relación a la existencia de causa de fuerza mayor.

2.- Alega la empresa demandante que ningún otro motivo sobre el fondo del asunto se contiene en el recurso del Ministerio de Trabajo, de modo que debe ser confirmada la SAN que consideró que la demanda igualmente debía merecer favorable acogida, ya que concurría la fuerza mayor en que se funda el expediente de regulación temporal de empleo instado por la empresa.

Es cierto que, el recurso del Abogado del Estado no contiene un motivo separado destinado a combatir ese pronunciamiento, pero también consta que a partir de sus apartados 22 y ss., el Abogado del Estado alega que la concreta situación padecida por la empresa no puede considerarse en modo alguno como un caso de fuerza mayor, en virtud del cual la empresa reciba un beneficio económico con cargo a los fondos públicos por algo que ni era imprevisible ni era tampoco inevitable para una empresa de la actividad de la que aquí se trata, dedicada a la actividad del Contact Center o Telemarketing, consistente en el servicio de atención de llamadas telefónicas. A tal efecto, señala que la sentencia impugnada debería haberse atenido al contenido jurídico de la fuerza mayor que resulta del art. 1105 del Código Civil, tal como lo ha aplicado la jurisprudencia, citando la Sentencia de esta Sala de lo Social, 819/2019, de 27 de noviembre de 2019 (recurso 95/2018; FD cuarto, apartado 2), y las en ella citadas.

3. Como dijimos en nuestra sentencia 486/2024, de 19 de marzo (RC 115/2022):"La doctrina del Tribunal Constitucional sostiene que en el recurso de casación las exigencias formales adquieren una especial relevancia, pues los requisitos de esta naturaleza parecen consustanciales a ese instituto procesal, debiendo distinguir entre el rigor formal, que viene justificado por la naturaleza del mismo recurso, y un exceso formalista que no puede cumplir otra función que la de dificultar la utilización del instrumento procesal (sentencia del TC núm. 17/1985, de 9 de febrero)".

Y a continuación, con remisión a la STS 608/2021, de 8 de junio (rec. 83/2020), argumentamos: "No caben formalismos excesivos, pero tampoco desconocimientos de que hay que cumplir de modo razonable cuanto la norma procesal pide [...] el actual art. 210.2 LRJS disciplina el escrito de interposición del recurso, conteniendo las siguientes exigencias: 1) Se expresarán por separado cada uno de los motivos de casación. 2) Se redactarán con el necesario rigor y claridad. 3) Se seguirá el orden de los motivos del artículo 207. 4) Hay que razonar la pertinencia y fundamentación de cada motivo. 5) Hay que razonar el contenido concreto de la infracción o vulneración cometidas. 6) Hay que realizar mención precisa de las normas sustantivas o procesales infringidas. 7) En los motivos basados en infracción de las normas y garantías procesales, deberá consignarse la protesta, solicitud de subsanación o recurso destinados a subsanar la falta o trasgresión en la instancia, de haber existido momento procesal oportuno para ello y el efecto de indefensión producido".

En este caso, aplicada la anterior doctrina al caso, debemos concluir, a tenor del contenido del escrito de interposición del recurso de casación ordinario, que la parte recurrente ha cumplido los requisitos esenciales de dicho medio de impugnación. La recurrente razona la pertinencia y fundamentación de la impugnación del fondo de la cuestión e invoca los preceptos legales que considera vulnerados y desarrolla los argumentos jurídicos en los que apoya su pretensión. De esta forma, podemos admitir la existencia de una impugnación de la referida cuestión de fondo, al haber citado el precepto legal que estima vulnerado, así como con cita de la Jurisprudencia de esta Sala que estima infringida, todo ello de conformidad al art. 210.2 de la LRJS.

Si bien la misma norma procesal exige que se expresen por separado, con el necesario rigor y claridad, cada uno de los motivos de casación, por el orden señalado en el artículo 207, dicha formalidad legal no debe impedir el acceso al recurso, si como es el caso, se cumple de forma suficiente con lo estipulado a continuación en relación a la pertinencia y fundamentación de los mismos y el contenido concreto de la infracción o vulneración cometidas, haciendo mención precisa de las normas sustantivas o procesales infringidas, así como, en el caso de invocación de quebranto de doctrina jurisprudencial, de las concretas resoluciones que establezcan la doctrina invocada.

CUARTO. - 1. Ya sobre el fondo, la recurrente, en síntesis, entiende que la causa de fuerza mayor exige como requisito la imposibilidad de trabajar, aspecto que no ha quedado acreditado en los hechos probados, a la luz de las declaraciones de los trabajadores y la justificación documental aportada, ya que lo cierto es que la actividad ordinaria de la empresa se vio parcialmente afectada, pero los trabajadores estuvieron en todo momento a disposición de la empresa, ya sea presencialmente o teletrabajando, e informaron a la empresa sobre sus descansos, comienzo y final de la jornada, así como de citas médicas para poder ausentarse de su puesto de trabajo, todo según consta en el expediente y en los HH.PP. (vid. el HP 6.º y la documentación remitida en él).

Añade que, tampoco concurren las notas que definen la fuerza mayor, esto es, la de ser una "circunstancia imprevisible e inevitable que impide el cumplimiento de una obligación". En tal sentido, señala que no se trata de un hecho imprevisible la posibilidad de un ataque informático que sufren continuamente las empresas, y menos tratándose de una empresa dedicada a la gestión de información sobre la utilización de sistemas tecnológicos e informáticos. Se trata de un riesgo eminentemente derivado de la propia realidad productiva

2. Como dijimos en nuestra STS 927/2021, de 22 de septiembre (RC 75/2021): "Con carácter general, el concepto de fuerza mayor, debe ser entendido como "un acontecimiento externo al círculo de la empresa y del todo independiente de la voluntad del empresario, que, a su vez, sea imprevisible" [STS (CA) de 23 de junio de 2003] y a los efectos de provocar una suspensión de los contratos de trabajo, (...); pero, sobre todo, que se trate de un acontecimiento no definitivo o sin vocación de permanencia que conlleve una simple imposibilidad temporal de que la prestación laboral se lleve a cabo [STS (CA) de 25 de julio de 1989]. Se trataría, en suma, de una imposibilidad temporal y sobrevenida de la prestación de servicios no imputable ni atribuible al empleador".

En STS de 22 de julio de 2015 (Recurso: 4/2012), dijimos que: "En su consecuencia, y como corolario de todo lo expuesto, ha de entenderse por fuerza mayor y, por ende, por "situación extraordinaria", un acontecimiento externo al círculo de la empresa, absolutamente independiente de la voluntad de ésta que sea imprevisible o, siendo previsible, sea inevitable, requisitos éstos, que no concurren en el presente caso".

3. El artículo 1105 del Código Civil cuando establece que: "Fuera de los casos expresamente mencionados en la Ley y de los en que así lo declare la obligación, nadie responderá de aquellos sucesos que no hubieran podido preverse, o que, previstos, fueran inevitables".

En resumen, recogiendo los criterios de la Sala primera, esta Sala ha señalado en la sentencia antes mencionada de 22 de julio de 2015, que por fuerza mayor debe entenderse "aquellos hechos que aun siendo previsibles, sean sin embargo inevitables, insuperables e irresistibles, siempre que la causa que los motiva sea independiente y extraña a la voluntad del sujeto obligado" (...) También se ha hecho referencia a este elemento como "sucesos imprevistos e inevitables que rebasan los tenidos en cuenta en el curso normal de la vida y extraños al desenvolvimiento ordinario de un proceso industrial"

La imprevisibilidad no es preciso, pues, que concurra, siendo suficiente con el hecho de que, siendo previsible, sea inevitable. En todo caso, no se discute, ni siquiera por la propia empresa demandante, el carácter previsible del ciberataque ni tampoco el que se trate de un hecho externo al círculo de la empresa.

En segundo lugar, la afirmación de que un ataque de ciberseguridad sufrido por una empresa, cuya prestación se desarrolla mediante el uso de sistemas informáticos, software, aplicaciones, etc., no pueda ser calificado de fuerza mayor, sino en todo caso una causa técnica o productiva, no es admisible, pues el hecho de que sea previsible un ataque de este tipo en una empresa cuyos medios materiales son esencialmente digitales, como lo son los ordenadores, no lo convierte en evitable.

Tampoco puede cuestionarse la existencia de fuerza mayor por el hecho de que el "suceso" no haya sido uno de los tradicionalmente considerados como tales, esto es, un incendio o un terremoto, pues el art. 1.105 CC no exige que sea un suceso natural, puede ser de otro tipo, atendida la realidad social en la que nos hallamos, una sociedad tecnológica, donde los sucesos pueden ser provocados por la acción del hombre. En ese sentido, la principal diferencia entre una causa de fuerza mayor y otra de tipo objetivo técnica no está en la causalidad natural de la primera y humana en la segunda, sino en el hecho de que la fuerza mayor es un suceso externo, ajeno a la voluntad de la empresa y de carácter extraordinario, y la segunda es una causa introducida, favorecida o exigida por las circunstancias, pero siempre ordinaria y voluntaria. La empresa puede haber previsto en su actividad ordinaria la existencia de un ciberataque (previsibilidad), pero hay algunos sucesos de este tipo que rebasan los tenidos en cuenta en el desenvolvimiento ordinario y, por ello, no pueden ser evitados (inevitabilidad). Por eso, si se trata de un suceso inevitable, que rebasa los que pueden ser tenidos en cuenta en el curso normal de la vida de la empresa, estaremos ante un supuesto de fuerza mayor.

4.- En el terreno de lo inevitable, los hechos probados ponen de manifiesto que la empresa había previsto la posibilidad de un ciberataque, ya que disponía de las medidas de seguridad necesarias y suficientes para evitar un ataque de ciberseguridad y, pese a ellas, el mismo no pudo ser evitado, como pone de manifiesto el Informe técnico aportado (documento núm. 6) y cuyo contenido está incorporado al relato fáctico en el sentido de que: "es muy complicado mantener una protección total ante la incidencia de este tipo de malware" y que "grandes instituciones nacionales e internacionales han sido atacadas por este tipo malware instituciones y empresas que, a pesar de contar con grandes medidas de seguridad en sus sistemas y la concienciación de sus usuarios, han sido víctimas de esta extorsión no pudieron ser evitados", o también que "es imposible mantener una protección total ante una incidencia de este tipo" (hecho probado quinto que da por reproducida la Memoria explicativa de las causas e informe técnico que se acompañaban a la misma como documentos 5 y 6, que obran en el expediente administrativo y en los descriptores 28 y 29, que se dan por íntegramente reproducidos).

En cuanto a las medidas de seguridad, el Informe afirma que: "La división ILUNION Contact Center BPO, (...), aplica una política de seguridad de la información completa y al más alto nivel tecnológico, que le ha hecho ser merecedora de las certificaciones ISO/IEC 27001 e ISO/IEC 27002, pese a ello el incidente se ha producido, lo que claramente demuestra la naturaleza de fuerza mayor del mismo, pues el mismo, como se ha comprobado, excede de la propia previsión y diligencia de la empresa". También se indica y así se recoge en los hechos probados que el sistema "no detecta o refiere brechas o fallos en la adopción de medidas preventivas por la Empresa y señala como prueba evidente, no solo

de la rigidez del sistema de seguridad existente en la Empresa, sino también de la efectividad de las medidas adoptadas por la Empresa es que, pese a la actividad ilegítima sufrida en los servidores, la exfiltración de información de la organización se considera muy baja".

De este modo, como se declara probado, el incidente se produjo, pese a las políticas de seguridad de la información existentes no solo a nivel organizativo, pues se declara probado que la Empresa dispone de una Política de Seguridad (PO01) de la cual se derivan normas que cubren todos los capítulos que se desarrollan en la ISO 27002, sino a nivel de la seguridad física de las instalaciones (se dice que, en especial, las relativas a los controles que regulan la seguridad en la operativa diaria sobre los sistemas de información, que comprenden la asignación nominativa de usuarios con exigencia de contraseñas complejas para su *login*; revisión periódica de los permisos y privilegios de los usuarios, con énfasis en aquellos usuarios administradores; segmentación de redes destinadas a servicios diferenciados; gestión de conexiones remotas seguras; programa antivirus actualizado en todos los equipos, gestionado de forma centralizada; realización periódica de copias de seguridad y almacenamiento en lugares seguros).

Se declara probado también que: "El ciclo de desarrollo de software, así como de su adquisición a terceros, está fundamentado en protocolos robustos que exigen el desarrollo seguro, con garantías de actualización periódica y en los casos en que sea aplicable, auditorías específicas de hacking ético. Se tiene una plataforma de trabajo extendida a todos los miembros de la organización, para la gestión integral de incidentes, mediante la cual se mantiene un flujo de trabajo controlado y documentado de todos los eventos que pueden afectar la seguridad de la información en la empresa. Tiene apoyo en empresas de soporte especializadas y realiza auditorías por una empresa independiente, Deloitte. Tiene Antivirus Kaspersky en todos los portátiles y ordenadores de sobremesa, así como en los servidores de toda la división; Firewall para el control y autorización de tráfico e IDS de la empresa Fortinet en el perímetro de seguridad del Centro de Procesamiento de datos, que realizan un filtrado de las conexiones y análisis del caudal de tráfico de entrada y salida de Contact Center".

En cuanto a que el suceso se habría evitado de haber tenido una copia de seguridad o un segundo CPD, como alega CGT, lo cierto es que, como consta probado, el *ransomware* es un programa de software malicioso que puede infectar un equipo o una red, cifrando la información y que los métodos de entrada de este malware son variados: mediante un enlace malicioso en una página web o la infección de un fichero compartido, siendo el más habitual el *phishing*, es decir, a través de los ordenadores de los propios usuarios, en este caso, trabajadores. De hecho, no se pudo conocer la vía de entrada, pero consta que ya desde el principio, a las 08:53 a.m. del día 4 de junio, Deloitte -experto independiente- procede a la activación del equipo de Respuesta e inicia el análisis forense comenzando por un equipo aislado de la red que se identifica como infectado. Se añade que: "(...) buscan en dicho portátil artefactos infectados por el malware y se concluye por la extensión de los archivos que se trata del ransomware RYUK".

De este modo, si el virus afectó a un equipo portátil el mismo día del ataque, como se dice, la duplicación del CPD no hubiera impedido el ataque.

6. - En cuanto a la imposibilidad objetiva de prestar servicios por parte de las personas trabajadoras, la CGT afirma que los trabajadores siguieron prestando su actividad mediante su puesta a disposición del empleador durante toda su jornada. El Abogado del Estado también insiste en esa idea y afirma que la actividad ordinaria de la empresa se vio parcialmente afectada, pero los trabajadores estuvieron en todo momento a disposición de la empresa, ya sea presencialmente o teletrabajando, e informaron a la empresa sobre sus descansos, comienzo y final de la jornada.

La propia ITSS, a partir de las declaraciones de algunos trabajadores, también afirmó que: "los trabajadores han estado en todo momento a disposición de la empresa, ya sea presencialmente o teletrabajando, y han informado sobre sus descansos, comienzo y final de la jornada, así como de citas

médicas para poder ausentarse de su puesto de trabajo" de lo que no cabe concluir que existiera efectiva prestación de servicios", de modo que lo único acreditado

El hecho de estar a disposición no es equivalente a prestación de servicios. Lo que aquí procede analizar es si realmente existió la imposibilidad de trabajar, no si los trabajadores estuvieron en disposición de trabajar, lo que en todo caso podría determinar que ese tiempo debería ser considerado tiempo efectivo de trabajo y, por tanto, retribuido, lo que es cosa distinta a la que ahora nos ocupa, cuál es la de determinar si pudieron trabajar de forma efectiva.

Además, el total de la plantilla de la empresa es de 2.158 personas (según consta en la Memoria, descriptor 28, en los centros de Madrid, Barcelona, Sevilla, Loroño y Jaén), de modo que se trata de un número muy superior al total de equipos afectados (1.200). De hecho, el número de trabajadores que la empresa computa como incluidos en el ERTE por fuerza mayor fue inferior al de los equipos afectados, en concreto de 1.192 personas, de modo que la afectación no fue total, sino parcial, esto es, que hubo trabajadores que pudieron seguir prestando servicios, como indica el Informe de la ITSS.

Cabría distinguir, por tanto, entre los trabajadores que quedaron a disposición de la empresa, sin poder trabajar y los que pudieron seguir prestando servicios, pese a todo, lo que concuerda con las manifestaciones de dos trabajadoras entrevistadas por la ITSS, al recoger que: "En cuanto a las manifestaciones de la parte social señalan que si bien no han trabajado con normalidad, ningún día han dejado de trabajar, encontrándose a disposición de la empresa, y registrando su jornada de trabajo tanto al principio como al final a través de t *eams*. Por ejemplo, Dña. Sara adscrita a la campaña de Renfe manifiesta que ningún día ha dejado de trabajar, de hecho, señala que tenía que estar presente en su puesto de trabajo, aunque es cierto que no ha trabajado con normalidad ni ella ni el resto de los compañeros adscritos a esta campaña. Sin embargo, tal y como puede comprobarse con posterioridad con el Excel de personal afectado presentado por la empresa la Sra. Sara está incluida en el expediente entre el 4 y el 7 de junio, y el 11 y 16 de junio. En el mismo sentido se manifiesta Dña. Vanesa, poniendo de relieve que desde el principio los trabajadores han estado prestando servicios, no ha habido paralización de la actividad. Señala además que han tenido que notificar los periodos de pausa o descanso".

En suma, no puede afirmarse, como hace la CGT, que todos los trabajadores siguieron prestando su actividad con normalidad, ya que lo único que consta es que algunos pudieron hacerlo, pero la mayoría simplemente quedó a disposición de la empresa, siendo que el número de trabajadores incluidos en el ERTE es inferior al de los equipos afectados y, muy inferior, también, a la plantilla de la empresa.

Ello se corrobora cuando los hechos probados afirman que con fecha 4 de junio de 2021 se suspendieron la mayor parte de los servicios que se prestaban a los clientes, quedando con ello sin actividad los empleados vinculados a dichas campañas, ante la imposibilidad de uso de las herramientas informáticas esenciales para el desarrollo de la actividad laboral y que, concretamente, se han visto afectadas por el ciberataque 28 campañas desarrolladas para distintos clientes (las mismas se reseñan en la Memoria-descriptor 28).

Consta asimismo que el CPD se apagó por completo y se procedió a cortar las comunicaciones con todas las sedes de la división Contact Center BPO para evitar la distribución del virus, mientras se desarrollaba la investigación forense del escenario identificado. De este modo, no existió tráfico saliente desde la organización a otros posibles servicios, ya que la red se encontraba completamente aislada y se remitieron comunicaciones a los clientes sobre el ciberataque producido y la imposibilidad de prestación de los servicios (un total de 131 comunicaciones efectuadas a clientes acerca de la imposibilidad de continuar prestando servicios como consecuencia del ciberataque producido).

En definitiva, por las razones expuestas, se acredita la producción del suceso de carácter ajeno a la empresa, su inevitabilidad, así como una efectiva imposibilidad de trabajar. Como consecuencia de cuanto precede se impone la estimación parcial del recurso, considerando que no hubo silencio positivo, pero en cuanto al fondo, procede confirmar la decisión de instancia que apreció la existencia de causa mayor.

QUINTO. - Por lo expuesto, y de conformidad con lo informado por el Ministerio fiscal, procede estimar parcialmente el recurso, confirmando en parte la sentencia recurrida, sin imposición de costas a la recurrente, a tenor del art. 235.2 de la LRJS, al haber estimado en parte su recurso.

F A L L O

Por todo lo expuesto, en nombre del Rey y por la autoridad que le confiere la Constitución, esta Sala ha decidido:

1.º.- Estimar en parte el recurso de casación interpuesto por el Abogado del Estado, en la representación que tiene de la Administración General del Estado (Ministerio de Trabajo y Economía Social), contra la Sentencia núm. 37/2022 de la Sala de lo Social de la Audiencia Nacional de 14 de marzo de 2022 en el procedimiento n.º 13/2022, sobre impugnación de actos administrativos en materia laboral y de seguridad social.

2.º. Casar y anular en parte la sentencia núm. 37/2022 de la Sala de lo Social de la Audiencia Nacional de 14 de marzo de 2022 en el procedimiento núm. 13/2022 y, desestimar la demanda en relación a la pretensión de nulidad de la Resolución de 15 de julio de 2021, por extemporánea, sin que proceda entender estimada por silencio la solicitud de ERTE por fuerza mayor de la empresa demandante y, confirmar en cuanto al fondo la misma, en el sentido de reconocer y constatar expresamente la concurrencia de fuerza mayor habilitando a la empresa a la adopción de las medidas suspensivas reconocidas en el artículo 47 del ET respecto de los trabajadores afectados.

3.º.- Acordar la no imposición de costas.

Notifíquese esta resolución a las partes e insértese en la colección legislativa.

Así se acuerda y firma.