Audiencia Nacional, Sala de lo Social, Sentencia 67/2023 de 26 May. 2023, Rec. 14/2022

Ponente: Aramendi Sánchez, José Pablo

Ponente: Aramendi Sánchez, José Pablo.

LA LEY 109238/2023

ECLI: *ES:AN:2023:2645*

ERTE. FUERZA MAYOR. Suspensión de contratos causada por un ataque informático. Silencio administrativo. La resolución adoptada denegatoria lo fue fuera del plazo legal por lo que opera que la solicitud sea estimada por silencio administrativo de efectos positivos. Ha quedado acreditado la relevancia del ataque informático y la afectación que produjo en la actividad empresarial tuvo la suficiente contundencia para operar como causa obstativa plena y determinante de la imposibilidad de trabajar. Se trata de un suceso previsible pero inevitable pese a contar la empresa con todas las herramientas de seguridad informática exigibles.

La Audiencia Nacional estima la demanda formulada por la mercantil y anulamos y dejamos sin efecto la resolución expresa adoptada por la Dirección General de Trabajo por la que se declaraba no constatada la existencia de fuerza mayor en la solicitud de suspensión de contratos de trabajo.

A Favor: EMPRESA.

En Contra: ADMINISTRACIÓN DEL ESTADO.

AUD.NACIONAL SALA DE LO SOCIAL

MADRID

SENTENCIA: 00067/2023

AUDIENCIA NACIONAL

Sala de lo Social

Letrada de la Administración de Justicia

Dª MARTA JAUREGUIZAR SERRANO

SENTENCIA Nº 67/2023

Fecha de Juicio: 23/05/2023

Fecha Sentencia: 26/05/2023

Tipo y núm. Procedimiento: IMPUGNACION DE ACTOS DE LA ADMINISTRACION 0000014 /2022

Ponente: JOSE PABLO ARAMENDI SÁNCHEZ

Demandante/s: ILUNION CEE CONTACT CENTER, S.A.U

Demandado/s: MINISTERIO DE TRABAJO Y ECONOMIA SOCIAL, CGT

Resolución de la Sentencia: ESTIMATORIA

Breve Resumen de la Sentencia:

AUD.NACIONAL SALA DE LO SOCIAL

-

GOYA 14 (MADRID)

Tfno: 914007258

Correo electrónico:

Equipo/usuario: MAD

NIG: 28079 24 4 2022 0000014

Modelo: ANS105 SENTENCIA

IAA IMPUGNACION DE ACTOS DE LA ADMINISTRACION 0000014 /2022

Procedimiento de origen: /

Sobre: IMPG. ACTOS ADMINISTRACION

Ponente Ilmo. Sr.: JOSE PABLO ARAMENDI SÁNCHEZ

SENTENCIA 67/2023

ILMO. SR.PRESIDENTE:

D. JOSE PABLO ARAMENDI SANCHEZ

ILMOS/AS. SRES./SRAS. MAGISTRADOS/AS :

D. RAMÓN GALLO LLANOS

Dª ANA SANCHO ARANZASTI

En MADRID, a veintiséis de mayo de dos mil veintitrés.

La Sala de lo Social de la Audiencia Nacional compuesta por los Sres./as. Magistrados/as citados al margen y

EN NOMBRE DEL REY

Han dictado la siguiente

SENTENCIA

En el procedimiento IMPUGNACION DE ACTOS DE LA ADMINISTRACION 14/2022 seguido por demanda de ILUNION CEE CONTACT CENTER, S.A.U (Letrado D. Juan José Jiménez Remedios) contra MINISTERIO DE TRABAJO Y ECONOMIA SOCIAL (Abogado del Estado D. Ignacio Landa Colomina), CGT (Letrado D. José María Trillo-Figueroa Calvo) sobre IMPG. ACTOS ADMINISTRACION. Ha sido Ponente el Ilmo. Sr. D. JOSÉ PABLO ARAMENDI SÁNCHEZ.

ANTECEDENTES DE HECHO

Primero.- Con fecha 14/01/22 se presentó demanda en materia de IMPG. ACTOS ADMINISTRACION promovida por el representante legal de ILUNION CEE CONTACT CENTER, S.A.U contra MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL, en la que, se dictó Sentencia con fecha 8/04/22, la cual fue recurrida en casación por el MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL y por CGT, elevándose las actuaciones al Tribunal Supremo con fecha 6/09/22.

Segundo.- Con fecha 30/03/23 se ha recibido en esta Sala la Sentencia del Tribunal Supremo nº 140/23 de fecha 20/02/23 en la que se acuerda: *"Declarar la nulidad de dicha Sentencia y de todas las actuaciones practicadas desde el momento de admisión a trámite de la demanda, para que se dicte una nueva resolución de admisión en la que se tenga por parte demandada al sindicato CGT y se le emplace para comparecer en el acto de juicio, continuando las actuaciones conforme a los trámites legalmente previstos".*

Se admite a trámite la demanda y de conformidad con lo dispuesto en art. 151.2 de la L.R.J.S., se señala el acto de conciliación el próximo día 23/05/23.

Tercero.- Llegado el día y la hora señalados tuvo lugar la celebración del acto de juicio, previo intento fallido de avenencia, y en el que se practicaron las pruebas con el resultado que aparece recogido en el acta levantada al efecto.

Cuarto.- Se ratifica ILUNION en la demanda y además hace referencia al informe de la UCO de la Guardia Civil sobre el virus padecido, que está en suspenso una reclamación patrimonial al Estado y que los trabajadores no vieron suspendidos sus contratos y se les abonó el salario y se pagaron las cotizaciones a la Seguridad Social.

Se opone la Abogacía del Estado alegando que la resolución impugnada se dictó dentro de plazo y que el silencio en todo caso es negativo. En cuanto al fondo del asunto sostuvo que no concurre fuerza mayor al tratarse de una empresa del ámbito de las telecomunicaciones, a la que es exigible una especial diligencia, que la aparición del virus no determinó el cese de la actividad.

CGT se opone a la demanda por las mismas razones expone que el funcionamiento ordinario de la empresa no se vio afectado, que existía previsibilidad de un ataque informático y la empresa no actuó con la diligencia debida ya que carecía de copias de seguridad fuera del entorno de red y si las hubiera tenido se habrían evitado las consecuencias del ataque.

Resultado y así se declaran, los siguientes

HECHOS PROBADOS

PRIMERO.- ILUNION CEE CONTACT CENTER S.A.U. es una sociedad perteneciente al grupo ILUNION, participado por la Fundación ONCE, dedicada a la actividad del Contact Center que consiste 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. Cuenta con cuatro centros de trabajo, en Madrid, Sevilla, Santander y Oviedo.

SEGUNDO.- El 21-6-2021 solicitó suspensión de los contratos de trabajo de 654 trabajadores de los 886 que componen su plantilla 480 empleados en el centro de Madrid, 152 en Barcelona y 22 en Santander. La causa invocada fue una incidencia informática causada por el ataque de un virus ransomware que se conoció el 4-6-2021 y que determinó aislar la red con el apagado completo de la CPD para frenar la expansión, lo que provocó el cese de la actividad de los 654 trabajadores para los que se solicita suspender contratos por fuerza mayor. D5 EX

A la solicitud acompañaba memoria, informe técnico y comunicaciones enviadas a la RLT sobre la solicitud de suspensión de contratos. Todos ellos que obran a los D 1, 2 y 3 del EX se dan por reproducidos.

En cuanto a la duración de la suspensión de contratos se indica en la memoria que deberá ser hasta que se haya conseguido reestablecer totalmente la actividad, todo ello sin perjuicio del compromiso de la Empresa de ir desafectando de manera paulatina al mayor número de trabajadores posible a medida que se vaya recuperando la actividad.

Se diseña en dicha memoria una planificación para la recuperación de la actividad en 14 semanas.

TERCERO.- La Dirección General de Trabajo, dio trámite de audiencia a los sindicatos e interesó el 9-7-2021 informe de la ITSS que se emite el 14-7-2021 desfavorablemente la solicitud y que al día siguiente se comunica a ILUNION.

El 15-7-2021 se dictó resolución por la Directora General de Trabajo en la que acuerda: Declarar no constatada la existencia de fuerza mayor en el expediente de presentado por la empresa ILUNION CEE CONTACT CENTER, S.A.U., con la consecuencia de denegar la solicitud formulada para la suspensión del contrato de trabajo de 654 trabajadores de su plantilla y demás inherentes a dicha declaración, sin perjuicio del derecho del interesado de iniciar el oportuno procedimiento por otras causas conforme a lo previsto en el artículo 33.4 del Reglamento de los procedimientos de despido colectivo y de suspensión de contratos y reducción de jornada, aprobado por Real Decreto 1483/2012, de 29 de octubre.

CUARTO.- La resolución se comunica a ILUNION el 19-7-2021 y por la demandante se presenta recurso de alzada el 13-8-2021. El 6-9-2021 se emite informe por el Subdirector General de Relaciones Laborales que se da por reproducido.

No se llegó a resolver de forma expresa el recurso de alzada.

QUINTO.- El día 4 de junio de 2021 a las 5:15 a.m. se recibió una incidencia en ILUNION CONTACT CENTER informando que los servicios de VDI (tecnología de virtualización de escritorio que almacena un sistema operativo en un servidor centralizado de un centro de datos) no funcionaban correctamente, se contactó con la compañía que da soporte, Unified Cloud Services (UCS), para identificar el problema y aplicar una solución. Posteriormente se detecta que un servicio de Base de Datos tampoco funciona correctamente.

A las 6:02 a.m. UCS informa que se está generando tráfico hacia ellos y que sospecha que

se trata de un virus ransomware y a las 6:40 a.m. se apaga el CPD (Centro de Proceso de Datos) completo y se procede a cortar las comunicaciones con todas las sedes de Contact Center para evitar la distribución.

Se informa del incidente a Grupo Ilunion y se convoca al Grupo de Respuesta ante incidentes de Ilunion (GRI), formado por los CIOs de Ilunion y 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 Deloitte, decidiendo activar el incidente en la póliza de ciberseguridad del Grupo.

Se inicia el análisis forense con la ayuda del equipo de Deloitte, comenzando por un equipo aislado de la red que se identifica como infectado. Se buscan en este 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.

Durante la mañana del viernes, 4 de junio, fue comunicado a la Agencia Española de Protección de Datos (AEPD) la brecha de seguridad sufrida. Dicha comunicación fue actualizada el domingo, 6 de junio.

SEXTO.- El ciber incidente sufrido impactó sobre todos los componentes que dependen de la Infraestructura informática empresarial, y, en consecuencia, se resintió la prestación de servicios por la imposibilidad de los agentes de utilizar los programas computacionales para operar los

servicios de contact center y gestión documental en todas las sedes. En el momento del incidente, se encontraban operando en el CPD corporativo (servicios básicos de red, autentificación, procesos, cti, base de datos y aplicaciones), así como en las diferentes sedes de la organización, de los que 114 fueron afectados y por lo tanto quedaron

inoperativos por este incidente. Del mismo modo, todas aquellas computadoras que estaban instaladas en las diferentes sedes de la compañía fueron afectadas por el incidente, quedando totalmente inoperativas (1200 equipos diferentes).

La ejecución del virus Ryuk, se inició de forma programada y coordinada en todos aquellos sistemas que pudieran ser objeto del virus (servidores y computadoras). El comportamiento del virus se inicia desinstalando de forma centralizada todas las soluciones antivirus existentes en los diferentes equipos afectados, para no ser detectado, y en ese momento comienza a encriptar todos los sistemas de ficheros existentes y accesibles desde cada máquina/servidor con sistema operativo Microsoft Windows (en todas sus versiones), sustituyendo su contenido original por contenido encriptado y su extensión por ".ryk"

No resultaron afectados aquellos servicios que se prestaban desde la infraestructura informática aportada por los propios clientes.

SÉPTIMO.- Se diseñó por ILUNION el proceso de recuperación de los sistemas afectados y del desarrollo habitual de la actividad, planificándose la realización de las tareas precisas en un periodo de 14 semanas y a partir de la recuperación de la información contenida en las copias de seguridad externas al sistema.

OCTAVO.- Los análisis realizados sobre el ataque informático padecido por ILUNON no han podido detectar la vía por la que el virus malicioso entró en el sistema operativo infectando los servidores y demás dispositivos.

NOVENO.- ILUNION Contact Center BPO, tiene implantado un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la necesidad de que la Seguridad de la Información esté en continua evolución y que dicha evolución en la madurez esté documentada y pueda ser verificada.

Desde 2017, cuenta con la certificación ISO/IEC 27001 de técnicas de seguridad de la información, otorgada por AENOR, y que es renovada anualmente mediante auditorías. Esta norma plantea un marco de gestión para llevar el sistema de gestión, y se complementa con la ISO/IEC 27002, que desarrolla controles específicos distribuidos en 13 capítulos, que suman 133 controles.

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.

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. La empresa cuenta con una Política de Seguridad (PO01) de la cual se derivan normas que cubren todos los capítulos que se desarrollan en la ISO 27002.

Existen, asimismo, 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.

Cuenta también con un procedimiento de gestión de incidentes de seguridad informática. La versión de 23-4-2020 era la existente al momento del ataque del virus. Emplea el antivirus Kaspersky en todos los dispositivos y servidores.

El 25-1-2021 se había elaborado por ILUNION un manual de respuesta técnica frente a ataques por ransomware.

Y tiene contratado con Telefónica un servicio de seguridad informática mediante cortafuegos Fortinet.

DÉCIMO.- En estas actuaciones se dictó sentencia por este tribunal el 8-4-2022. Su contenido se da por reproducido.

La citada sentencia fe recurrida en casación y el Tribunal Supremo se pronunció el 20-2-2023, rec. 193/22, declarando *la nulidad de la sentencia y de todas las- actuaciones practicadas desde el momento de admisión a trámite de la demanda, para que se dicte una nueva resolución de admisión en la que se tenga por parte demandada al sindicato CGT y se le emplace para comparecer en el acto de juicio, continuando las actuaciones conforme a los trámites legalmente previstos.*

Se han cumplido las previsiones legales.

FUNDAMENTOS DE DERECHO

PRIMERO.- Los hechos se declaran probados atendiendo a los siguientes elementos de convicción:

- hecho 1º: no es controvertido

- hecho 2º. 3º y 4º: se obtienen de las actuaciones y resoluciones obrantes en el expediente administrativo

- hecho 5º: de acuerdo con la memoria e informe técnico aportados con la solicitud de suspensión y que obran a loa D26 y 27 y han sido reconocidos de adverso

- hecho 6º: conforme la memoria y el informe técnico referidos y conforme el testimonio del Sr. Luis que revela la no afectación de entornos ajenos a Ilunion

- hecho 7º: se obtiene del informe técnico

- hecho 8º: se obtiene de los informes técnicos, de Deloitte y de la UCO al D 206

- hecho 9º: se obtiene de los datos contenidos en la memoria y a los D 35, 36 y 69

- hecho 10º: conforme las precedentes sentencias que obran en las actuaciones.

SEGUNDO.- Se cuestiona por la demandante la nulidad de la resolución expresa denegatoria de la suspensión de contratos por fuerza mayor, alegándose que dicho acto administrativo está dictado fuera de plazo y que debe aplicarse el art. 24.1 LPA determinante por silencio administrativo de la aprobación de la solicitud.

El art. 33.1 del RD 1483/2012 determina que en las solicitudes de suspensión de relaciones de trabajo y reducción de jornada por fuerza mayor se dictará resolución en plazo máximo de cinco días desde la fecha de entrada de la solicitud en el registro del órgano competente para su tramitación, lo que tuvo lugar en este caso el 21-6-2021.

Pero esta misma norma establece que *la autoridad laboral competente recabará, con carácter preceptivo, informe de la Inspección de Trabajo,* lo que determina que deban aplicarse las prevenciones establecidas en el art. 22 LPA conforme el cual el plazo máximo para resolver y notificar la resolución **podrá suspenderse...***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*.

La suspensión cobra sentido si los informes se solicitan dentro del plazo con el que cuenta la Administración para resolver, pero no en el caso de que dicha solicitud tenga lugar ya sobrepasado el plazo resolutorio.

En el caso presente queda acreditado que la solicitud del empresario para suspender contratos por FM se lleva a cabo el 21-6-2021. Contaba la Administración con un plazo de cinco días para dictar resolución, plazo que finalizaba el 28-6- 2021. Dado que tal como consta en el expediente administrativo, el informe a la ITSS se solicita el 9-7-2021 ya se había sobrepasado holgadamente el plazo de cinco días para resolver por lo que la citada solicitud no puede servir de instrumento suspensivo de dicho plazo.

TERCERO.- El art. 24.1 LPA dispone que *En los procedimientos iniciados a solicitud del interesado, sin perjuicio de la resolución que la Administración debe dictar en la forma prevista en el apartado 3 de este artículo, el vencimiento del plazo máximo sin haberse notificado resolución expresa, legitima al interesado o interesados para entenderla estimada por silencio administrativo.*

Esta norma recoge una serie de supuestos contrarios a la aplicación de esta regla general en favor del silencio positivo y por tanto resoluciones por silencio con efectos negativos, a saber: concurrencia de norma europea o internacional que establezca lo contrario, acceso a actividades o su ejercicio, ejercicio derecho de petición aquellos cuya estimación tuviera como consecuencia que se transfirieran al solicitante o a terceros facultades relativas al dominio público o al servicio público que impliquen el ejercicio de actividades que puedan dañar el medio ambiente y en los procedimientos de responsabilidad patrimonial de las Administraciones Públicas y procedimientos de impugnación de actos y disposiciones y en los de revisión de oficio iniciados a solicitud de los interesados.

La suspensión de contratos de trabajo con causa en FM no encaja en ninguno de estos supuestos que excepcionan el valor positivo del silencio administrativo, por lo que se debe llegar a la conclusión de que la posterior resolución dictada el 15-7-2021 es nula y carece de efectos, debiendo sustituirse por la validación administrativa por silencio de la solicitud suspensiva de contratos.

En esta línea argumental debe citarse la STS 25-1-2021 rec 125/20, invocada por la parte demandante si bien se trataba de un supuesto aplicando el art 22.2.c del RDL 8/2020 de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19, lo que no es el caso.

CUARTO.- En todo caso y por si no se apreciase que la solicitud suspensiva de contratos fue estimada por silencio positivo por la administración autorizante, pasaremos a continuación al análisis de la cuestión de fondo.

El art. 4.2.a) ET reconoce como un derecho básico del trabajador el de la ocupación efectiva. Tratándose de un contrato sinalagmático la ocupación efectiva y consiguiente prestación de servicios al empresario se corresponde con la obligación para éste, art. 4.2.f) ET, de abonarle la remuneración pactada.

Este devenir ordinario del contrato de trabajo y sus correspondientes obligaciones de trabajar y remunerar puede verse alterado por la concurrencia de supuestos fácticos que encajen en la llamada fuerza mayor, que incidiendo en el decurso del contrato, determine su suspensión, art 47.3 ET, o su extinción art. 51.7 ET.

No contiene el ordenamiento laboral una definición de la fuerza mayor por lo que, para su identificación, habrá de aplicarse el art. 1105 CC que dispone:

> *"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."*

Opera por tanto la fuerza mayor como un mecanismo que exonera del cumplimiento de las obligaciones, lo que trasladado al marco de las relaciones laborales se traduce en la imposibilidad

de trabajar, por la concurrencia de un suceso imprevisible o previsible pero inevitable, lo que exoneraría de la correlativa obligación de abonar el salario.

En este contexto, las previsiones del legislador pasan por establecer mecanismos de cobertura prestacional (la prestación por desempleo) de las retribuciones de los trabajadores. El hecho de comprometerse fondos públicos para atender la pérdida de salario, justifica la intervención administrativa con el objeto de constatar la concurrencia cierta de fuerza mayor.

QUINTO.- La resolución administrativa niega que en este caso concurra fuerza mayor con los siguientes argumentos:

- Que la empresa no aporta ninguna prueba documental que efectivamente acredite la existencia de un virus informático en su sistema

- que no ha quedado acreditada la imposibilidad de trabajar con causa en el ataque

- que se trata de un caso que se conoce como fuerza mayor impropia, respecto de los que exige la jurisprudencia que la fuerza mayor venga determinada por la existencia de acontecimientos extraordinarios, que **sean imprevisibles e inevitables** por parte del empresario. Es un riesgo previsible la posibilidad de un ataque informático atendiendo la actividad empresarial

Los dos primeros argumentos de carácter fáctico se basan en el informe de la ITSS.

Dicho informe en ningún caso niega el ataque padecido, como tampoco se niega en juicio por la Abogacía del Estado ni por CGT. El ataque está plenamente acreditado por el informe técnico también reconocido y por el informe de la UCO al 206. Es relevante que parte del informe técnico se vuelca en el informe de la ITSS para describir el acontecimiento determinante de la solicitud.

Sí indica el informe de la ITSS que *la causa de fuerza mayor suspensiva tiene como requisito la imposibilidad de trabajar, aspecto que no ha quedado acreditado a la luz de las declaraciones de los trabajadores y la justificación documental aportada por la parte social.*

Las declaraciones de los trabajadores se refieren a las manifestaciones realizadas a la Inspección por los representantes sindicales que 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 teams*.

Por ejemplo, Dña. Ana 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 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. Ana 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. Belen, 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.

Concluye de estas pruebas el informe de la ITSS que ILUNION no acredita que el ataque informático impidiera la prestación de servicios, por lo que no constituyó causa suficiente para impedir el cumplimiento de las obligaciones de trabajar y remunerar.

En la demanda, pág. 43 y sig, se trata de argumentar acerca de la relevancia obstativa (impeditiva para trabajar) que tuvo el ataque y en la pag. 58 se hace referencia a un hecho relevante y acreditado *la inutilización de servidores, sistemas electrónicos, computadoras (en número aproximado 1.200) e impresoras, afectando en un primer estadio a un total de 1.192 empleados*.

Por otra parte el informe técnico también revela que diseñó ILUNION el proceso de recuperación de los sistemas afectados y del desarrollo habitual de la actividad, planificándose la realización de las tareas precisas en un periodo de 14 semanas y a partir de la recuperación de la información contenida en las copias de seguridad externas al sistema.

Consideramos en consecuencia que dichos informes revelan con claridad la relevancia del ataque y la afectación que produjo en la actividad empresarial por lo que, pese el informe de la ITSS y atendiendo a las pruebas que lo soportan, llegamos a la conclusión de que efectivamente el ataque tuvo la suficiente contundencia para operar como causa obstativa plena y determinante de la imposibilidad de trabajar.

Cuestión distinta pero que escapa de este proceso, es la determinación de si la afectación tuvo la misma intensidad y duración para todos los trabajadores.

SEXTO.- Se manifiesta en la resolución, como acabamos de señalar que para la autoridad laboral no concurría fuerza mayor porque no se trató de un acontecimiento imprevisible e inevitable.

Evidentemente los ataques informáticos no pueden ser considerados acontecimientos imprevisibles pues su existencia está a la orden del día, pero el art. 1105 CC no aprecia la fuerza mayor en la concurrencia de imprevisión e inevitabilidad sino que la califica como la consistente *en aquellos sucesos que no hubieran podido preverse, o que, previstos, fueran inevitables*.

Por tanto, lo que debemos analizar en el presente caso es si el previsible ataque informático resultaba inevitable.

La evitabilidad o inevitabilidad de un suceso, al igual que acontece con los accidentes de trabajo, no impone la consecución necesaria de un resultado, en este caso que el ataque informático sea siempre neutralizado (como tampoco la legislación impone la obligación de que no se produzca un accidente laboral), sino que se hayan adoptado todas las medidas preventivas disponibles para su neutralización.

Y en el presente caso la prueba practicada es demostrativa de que ILUNION contaba con toda una serie de medios para atajar estos ataques, en lo racionalmente posible y conforme los conocimientos técnicos normalizados, tal como revela el HP 9º.

No se aprecia en este caso, porque tampoco se alega, una conducta defectuosa en sus obligaciones preventivas en materia de seguridad informática, por lo que debemos concluir de que pese a las adecuadas que se adoptaban por ILUNION el ataque tuvo lugar. Ataque que resultó ser de la suficiente sofisticación, al punto de no haberse podido aún acreditar pese a los informes técnicos y del UCO, cuál fue el mecanismo de entrada del virus en la intranet de la empresa.

Por todas estas razones la demanda debe finalmente resultar estimada.

SÉPTIMO.- Contra esta sentencia cabe recurso ordinario de casación conforme art. 206.1 LRJS.

VISTOS los preceptos legales citados y demás de general y pertinente aplicación,

FALLAMOS

ESTIMAMOS la demanda formulada por la mercantil ILUNION CEE CONTACT CENTER S.A.U y anulamos y dejamos sin efecto la resolución expresa adoptada por la DIRECCIÓN GENERAL DE TRABAJO el 15-7-2021 por la que se declaraba no constatada la existencia de fuerza mayor en la solicitud de suspensión de contratos de trabajo interesada por la demandante el 21-6-2021, solicitud que reconocemos con esta resolución.

Notifíquese la presente sentencia a las partes advirtiéndoles que, contra la misma cabe recurso de Casación ante el Tribunal Supremo, que podrá prepararse ante esta Sala de lo Social de la Audiencia Nacional en el plazo de **CINCO DÍAS** hábiles desde la notificación, pudiendo hacerlo mediante manifestación de la parte o de su abogado, graduado social o representante al serle notificada, o mediante escrito presentado en esta Sala dentro del plazo arriba señalado.

Al tiempo de preparar ante la Sala de lo Social de la Audiencia Nacional el Recurso de Casación, el recurrente, si no goza del beneficio de Justicia Gratuita, deberá acreditar haber hecho el depósito de 600 euros previsto en art. 229.1.b de la Ley Reguladora de la Jurisdicción Social, y, en el caso

de haber sido condenado en sentencia al pago de alguna cantidad, haber consignado la cantidad objeto de condena de conformidad con el art. 230 del mismo texto legal, todo ello en la cuenta corriente que la Sala tiene abierta en el Banco de Santander Sucursal de la Calle Barquillo 49, si es por transferencia con el (IBAN ES55) nº 0049 3569 92 0005001274 haciendo constar en las observaciones el nº 2419 0000 00 0014 22; si es en efectivo en la cuenta nº 2419 0000 00 0014 22, pudiéndose sustituir la consignación en metálico por el aseguramiento mediante aval bancario, en el que conste la responsabilidad solidaria del avalista.

Llévese testimonio de esta sentencia a los autos originales e incorpórese la misma al libro de sentencias.

Así por nuestra sentencia lo pronunciamos, mandamos y firmamos.