ADMINISTRACION DE JUSTICIA

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 nº 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 XXXXXX BPO. (descripción 34). El Mapa de la red XXXXXX 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 XXXX 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 XXXXXX 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.

ADMINISTRACION DE JUSTICIA

- El 9 de julio de 2021, se recibió requerimiento de documentación por parte de la Inspección de Trabajo y de la Seguridad Social, citando a la Empresa a comparecencia en fecha 13 de julio de 2021.
- El 15 de julio de 2021, se dicta la resolución recurrida por medio del presente por la Autoridad Laboral competente, siendo la misma notificada a la parte actora en fecha 19 de julio del año corriente.

Tal y como se sostiene en la demanda, fijados los elementos temporales esenciales, debe procederse a la revocación de la resolución íntegra toda vez que la misma resulta extemporánea y, de conformidad con lo previsto en el artículo 24.3 a) de la LPAC, en caso de estimación por silencio, las resoluciones extemporáneas de procedimientos iniciados a solicitud de interesado solo pueden ser confirmatorias de éste.

El artículo 33.1 del Real Decreto 1483/2012, dispone que la Autoridad Laboral dictará resolución en el plazo máximo de 5 días a contar desde la fecha de entrada de la solicitud en el registro del órgano competente para su tramitación (arts. 51.7 y 33.1 RPDC), y la notificará a la empresa interesada dentro del plazo de 10 días a partir de la fecha en que haya sido dictada (art. 40.2 LPAC). Dichos días, de conformidad con lo estipulado por los arts. 30 y 31 de la LPAC son hábiles.

No obstante, el plazo máximo legal para resolver el procedimiento y notificar la resolución se podrá suspender o ampliar en los términos previstos en los arts. 22 y 23 de la LPAC, respectivamente. En efecto, el art. 22 de la LPAC dispone que el transcurso del plazo máximo legal para resolver el procedimiento y notificar la resolución se podrá suspender en determinados supuestos, a saber:

[…] 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», y sin que este plazo de suspensión pueda «exceder 16 en ningún caso de tres meses» [art. 22.1.d) LPAC]. En caso de no recibirse el informe en el plazo indicado, proseguirá el procedimiento [art. 22.1.d) LPAC].

Cuando la autoridad no dictase y notificase resolución expresa en el plazo máximo de cinco más diez días previsto en los arts. 51.7 y 33.1del ET y del RPDC y 40.2 de la LPAC, ha de estarse a lo dispuesto en el art. 24.1 de la LPAC (silencio estimatorio o positivo). Ha de tenerse en consideración, a estos efectos, que en el ERTE por fuerza mayor el informe de la ITSS es preceptivo y no potestativo. Por tanto, si bien es cierto que el informe de la ITSS suspende conforme al artículo 22 LPAC el plazo de 5 días hábiles para resolver, conforme a la literalidad de la norma, deberá comunicarse al interesado dicha suspensión. Por tanto, dada cuenta de que no se ha efectuado dicha comunicación, en ningún caso podría haberse producido la suspensión del plazo para resolver de conformidad con los artículos citados.

Por tanto, en los casos de solicitudes de constatación de fuerza mayor, la falta de resolución en tiempo por parte de la Administración provoca efectos estimatorios de la misma, siendo esta conclusión previsión legal expresa conforme a lo previsto en el

ADMINISTRACION DE JUSTICIA

artículo 24.1 LPAC y, habiendo sido expresamente resuelto por el Tribunal Supremo en Sentencia de fecha 25 de enero de 2021,rec.125/2020, el cual se ha pronunciado sobre el sentido del silencio por parte de la Autoridad Laboral ante la solicitud de ERTE por causa de fuerza mayor afirmando que el mismo debe ser estimatorio o positivo. El caso analizado en la Sentencia de referencia se refiere a la decisión de distintos Ayuntamientos de distintas Comunidades Autónomas, de suspender el servicio de escuela infantil o guarderías municipales, acatando la orden de cierre de escuelas infantiles dictadas al inicio del Estado de Alarma. Ello provocó que las distintas empresas concesionarias del servicio de guardería municipal solicitasen ERTE por causa de Fuerza mayor, que fue aprobado por la Autoridad Laboral competente, pero de forma extemporánea -esto es, transcurrido el plazo legal de 5 días desde la solicitud por parte de la empresa-.

Concluye el TS sobre este aspecto, afirmando la aplicación del silencio positivo. Se afirma en dicha resolución que, "La *empresa cumplió con las exigencias del art. 22.2 del RD-L. 8/2020, por lo que nada impide que opere el silencio administrativo positivo. Cierto es que no se refiere a esta figura el RD-Ley 8/2020, de 17 de marzo , de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19, pero así resulta del Real Decreto-Ley 9/2020 de 27 de marzo , tanto en el preámbulo con remisión al art. 24 de la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas, de 1 de octubre (que como regla general, otorga al mismo sentido positivo, no encontrándonos ante un supuesto en el que se establezca lo contrario), como en el propio articulado en relación a la constatación de la fuerza mayor vinculada al COVID-19 para aplicar medidas temporales de suspensión de contratos de trabajo o de reducción de la jornada laboral , se deben entender estimadas por silencio administrativo positivo en el supuesto de que no se dicte una resolución expresa en el plazo de 5 días (artículo 22.2.c del RDL 8/2020)"* . Doctrina que es de aplicación al supuesto de autos con independencia de que la causa de fuerza mayor esté fundada en causa no asociada a la crisis sanitaria.

En este caso, desde que se efectúa la solicitud de constatación de fuerza mayor en fecha 21 de junio de 2021, hasta que se dicta resolución, fecha 15 de julio de 2021, transcurren un total de 18 días hábiles, y un total de 20 días hábiles hasta ser notificado, lo que excede, con creces el plazo de 5 días hábiles máximo para dictar resolución que habilita el meritado artículo 33.

Llegados a este punto, ha de resaltarse que en el Antecedente Quinto de la resolución denegatoria de la fuerza mayor se utiliza como elemento de justificación para la resolución extemporánea de la solicitud, el incidente de ciberseguridad sufrido a partir del día 9 de junio de 2021 por el Ministerio de Trabajo y Economía Social, que motivó el dictado de Resolución por parte de la Dirección General de Empleo, de fecha 16 de junio de 2021, por la que se ampliaban los plazos en el ámbito de actuación y funcionamiento hasta la resolución de las incidencias. Esto es, no se utiliza como argumento el posible retraso en que pudiera haber incurrido la Inspección de Trabajo en la evacuación de informe -que, entre otras cosas, no resultaría admisible dado que nada se comunicó a la demandante sobre la suspensión del plazo-, sino la cita expresa de la resolución de 16 de junio de 2021.

ADMINISTRACION DE JUSTICIA

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. Se adjuntan al presente Informe como Documentos nº 2, 3, 4 y 5, las comunicaciones realizadas a la AEPD.

El Ciber incidente sufrido en los sistemas ubicados en todas las sedes de la compañía, que tras las investigaciones y medidas necesarias se determinó que se debió al ransomware conocido como Ryuk, impactó sobre todos los componentes que dependen de esta infraestructura, y, en consecuencia, se resiente 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 26 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).

II. Del Informe forense elaborado por firma externa independiente, que se acompañaba como Anexo VIII del documento nº 6, anexionado a la solicitud inicial de constatación de fuerza mayor y el que se aportó en el curso del procedimiento administrativo (documento nº 2 de los acompañados al Recurso de Alzada informe definitivo que, asimismo, fue aportado a la Inspección de Trabajo en fecha 13 de julio de 2021). En el citado informe forense En el mismo se relataba exhaustivamente i) el ataque sufrido; ii) la suficiencia y adecuación de las medidas adoptadas por la Empresa y iii) el impacto del mismo en el normal funcionamiento de la Compañía.

Se efectúa específica valoración sobre las consecuencias del ataque, la imposibilidad de conocer el vector de entrada y la diligencia debida de la Compañía en el despliegue de las medidas de seguridad informática necesarias.

Tras el análisis de las máquinas adquiridas, se han identificado diversas piezas de malware asociadas al ransomware Ryuk.

ADMINISTRACION DE JUSTICIA

Respecto al vector de entrada empleado por los atacantes para el acceso a la organización, no ha sido posible evidenciarlo fehacientemente en base a los logs y artefactos digitales disponibles. Se valoran no obstante tres hipótesis posibles: (…)

Se efectuaron comunicaciones sobre la brecha de seguridad ocasionada, como consecuencia del ataque informático, a la Agencia Española de Protección de Datos. (adjuntas al informe técnico aportado en la solicitud de fuerza mayor (como anexo II a V) y obrante en el expediente administrativo.)

Se efectuaron comunicaciones a los clientes sobre el ciberataque producido y la imposibilidad de prestación de los servicios, que se acompañó a la solicitud de constatación de fuerza mayor como anexo XIII del documento nº 6 (informe técnico que se acompañó a la solicitud de fuerza mayor).

B) Sobre la concurrencia de causa de fuerza mayor derivada del bloqueo de los sistemas informáticos de la compañía como consecuencia del sufrimiento de ataque informático mediante virus ransoware, de conformidad con lo previsto en los artículos 47.3 et y 51.7 ET en concordancia con los previsto en los artículos 32 y 33.3 del Real Decreto 1483/2012 así como de la jurisprudencia que lo interpreta. adopción de medidas de seguridad diligentes e inevitabilidad del suceso.

La legislación laboral no recoge una definición de lo que debe entenderse por imposibilidad objetiva sobrevenida, aunque son diversos los preceptos que hacen referencia a la misma. Al margen de lo que se conoce doctrinalmente como derecho de la emergencia (fundamentalmente desarrollado como consecuencia de la crisis sanitaria derivada del Covid-19), el concepto "fuerza mayor" aparece de forma expresa en diversas disposiciones del ET (artículos 37.7, 45.1.i, 47.2 y 3, 49.1.h, 50.1.c, y 51.7) y, en otras ocasiones, también se hace referencia a supuestos en los que de forma sobrevenida, concurre un hecho obstativo imposibilitante que impide el cumplimiento de las prestaciones pactadas en el contrato de trabajo (artículos 45.1.c, 49.1.e y 49.1.g todos ellos del ET).

La Sala IV del Tribunal Supremo, en S. de 8 de julio de 2008 (rec. 1857/2007), sostiene: "*La fuerza mayor se configura en el marco de la regulación de los efectos del incumplimiento del contrato (artículo 1105 del Código Civil en relación con los artículos 1101, 1102, 1103 y 1104 del mismo texto legal) como un criterio de imputación (fuerza mayor y caso fortuito frente a culpa y dolo). (…) como muestran los antecedentes de la regulación actual - en concreto el artículo 76. 6ª LCT y el artículo 20 de la LRL -, lo que hay que determinar es si concurren los dos elementos que configuran el supuesto extintivo específico de los artículos 49.h) y 51.12 del Estatuto de los Trabajadores: la imposibilidad definitiva de la prestación de trabajo y el carácter de fuerza mayor de la acción que la determina".*

la STS, (Sala de lo Contencioso-Administrativo), de 19 de octubre de 1994 (rec 2949/1990), analizando el debate -entre fuerza mayor y caso fortuito, se concluye sobre las notas de imprevisibilidad o inevitabilidad que: "*La fuerza mayor es el suceso que está fuera del círculo de actuación obligado que no hubiera podido preverse o que, previsto, fuera inevitable, y en orden a su apreciación en el ámbito*

jurídico, se ha de tener en cuenta que aunque en el terreno doctrinal es opinión dominante, la que viene a identificar las figuras del caso fortuito y la fuerza mayor, algún sector de la doctrina entiende que existen diferencias entre uno y otra, y que en la fuerza mayor no sólo es imprevisible sino además inevitable o irresistible (vis cui resistiti non potest).”

La Sala IV del TS, en S. de 22 de julio de 2015, rec. 4/2012 ha definido la causa de fuerza mayor como: “*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.”*

Como recogen las sentencias del 7 de junio y 28 de septiembre de 1988 y 10 de noviembre del mismo año "*la fuerza mayor se caracteriza por dimanar de 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*" o como dice la del 3 de noviembre de 1988, en aplicación concreta al caso litigioso, el suceso "*no tuvo una causa externa o ajena al funcionamiento del servicio"*; y la sentencia de la Sala III de este Tribunal de 29 de junio de 1998 (recurso 4505/1992), dictada sobre exoneración de la cotización a la Seguridad Social como consecuencia de la suspensión de contratos de trabajo, señalaba que , "*Resulta de aplicación al supuesto que nos ocupa la Sentencia de esta Sala de 7 de marzo de 1995 , que define la fuerza mayor como un acontecimiento externo al círculo de la empresa y del todo independiente de la voluntad del empresario, que a la vez sea imprevisible. En el mismo sentido la Sentencia de 16 de mayo de 1995 , según la cual la fuerza mayor es un concepto jurídico indeterminado que comprende no solamente las causas a que se refería el art. 76.6 de la Ley de 26 de enero de 1944 del Contrato de Trabajo , sino a cualquier otra que dimane de un hecho externo ajeno a la esfera de actividad del empresario, doctrina acorde con la naturaleza de la fuerza mayor que en cada caso debe ser estimada o no, y que comporta que el hecho determinante del incumplimiento de una obligación, aunque pudiera preveerse, resulte inevitable*".

La doctrina judicial civilista, por todas, STS (Sala de lo Civil) de 22 de noviembre de 2018, ha anudado la circunstancia de fuerza mayor a:
“*Una fuerza superior a todo control y previsión que debe ponderarse -a efectos de su concurrencia- con la normal y razonable previsión que las circunstancias exijan adoptar en cada supuesto concreto.*” S

Sobre esta nota se ha entendido que debe procederse a una evaluación estudiándose la singularidad en cada caso concreto, pues, se trata de un concepto jurídico que debe deducirse del conjunto de circunstancias que motiven el hecho o acontecimiento que sobreponiéndose a la voluntad del obligado lo determinan a quebrantar la obligación que le corresponda, ya que siendo la posibilidad de prever los sucesos un concepto amplio, hay que entenderlo en su aplicación legal y práctica, como excluyente de aquellos sucesos totalmente insólitos o extraordinarios que, aunque no imposibles físicamente, no son de los que puede calcular una conducta prudente.

ADMINISTRACION DE JUSTICIA

Sobre la concurrencia de causa de fuerza mayor como consecuencia del ataque de virus ransomware en XXXXXXXX, S.A.U. El análisis de los elementos configuradores de la fuerza mayor de los apartados anteriores permite concluir que el ataque informático a través de un virus ransomeware que se traduce 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 efecto, concurren todos los elementos configuradores que permiten concluir la existencia de causa de fuerza mayor: imposibilidad, existencia de una relación causal entre el incumplimiento de la obligación contractual y el hecho obstativo, inimputabilidad y (al menos) inevitabilidad. Elementos aplicados a la situación concreta descrita en la solicitud de constatación de fuerza mayor, formulada por la empresa.

(i) Sobre la naturaleza del hecho obstativo: tal y como se describe en los hechos declarados probados, se produjo en fecha 4 de junio de 2021 un ataque informático deliberado (en este caso, en forma de ransomware) por parte de terceros ajenos a la Empresa.

Tal circunstancia, resulta subsumible en el concepto de fuerza mayor, el origen "humano" (e, incluso, "intencionado") del hecho obstativo, no es una circunstancia suficiente para descartar una posible concurrencia de una fuerza mayor.

(ii) Sobre la concurrencia de un hecho obstativo, resulta acreditado, y así se colige del contenido de los informes periciales, que el secuestro de datos que el cifrado provoca tiene una afectación claramente obstativa en el cumplimiento de las prestaciones contractuales acordadas. Especialmente porque imposibilita la oportunidad empresarial de ofrecer la prestación de trabajo a las personas trabajadoras, en la medida que se ha visto afectado el Centro de Procesamiento de Datos, en la división XXXXXXX BPO, se ha producido 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).

Esta circunstancia no puede quedar desvirtuada, por el informe de CGT cuyo contenido se incorpora parcialmente a la resolución de la Directora General de Trabajo, en el que se afirma que, los empleados quedaron a disposición de la empresa, siendo ello elemento suficiente para impedir la suspensión de sus contratos. El argumento no es admisible porque la mera manifestación de "disponibilidad" no es equivalente a la ocupación efectiva, cuando hay imposibilidad objetiva de prestar servicios laborales.

Es decir, las personas trabajadoras pueden manifestar estar disponibles para realizar actividad laboral, pero la disponibilidad se traduce en la manifestación del mero deseo de querer trabajar, pero sin poder hacerlo porque existe una causa, ajena a voluntad de empleados y empresa, que lo impide.

ADMINISTRACION DE JUSTICIA

(iii) Sobre la existencia de una relación de causalidad.- Existe una estrecha 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 , tal y como se acredita en informe técnico) del que se desprende que, el ciberincidente sufrido en los sistemas ubicados en todas las sedes de la compañía, que tras las investigaciones y medidas necesarias se determinó que se debió al ransomware conocido como Ryuk, impactó sobre todos los componentes que dependen de esta infraestructura, y, en consecuencia, se resiente 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).

(iv) Sobre la inimputabilidad y la imprevisibilidad o la inevitabilidad. -sin duda, estos son los elementos más determinantes de este supuesto. Y, por este motivo, conviene un análisis pormenorizado.

Para poder determinar esta cuestión es oportuno, evaluar si el riesgo era imprevisible o, si previsto, inevitable. Especialmente porque, en función de la naturaleza del hecho sobrevenido, podrá delimitarse la diligencia requerida a través del análisis de las medidas preventivas o de seguridad adoptadas (esto es, si se agotaron cuantas medidas de precaución incumben a la Empresa en la evitación de este fenómeno).

En primer lugar, no puede afirmarse que un ataque informático ni la afectación de un virus sean circunstancias totalmente imprevisibles (y el ransomeware tampoco), y en este sentido se pronuncia la Administración actuante, la Inspección de Trabajo y, la resolución recurrida.

Ahora bien, en este supuesto, concurren los factores suficientes para concluir que el nivel de diligencia empresarial para prevenir este riesgo ha sido adecuado conforme a lo que una "conducta prudente hubiera podido evaluar".

En efecto, atendiendo a la naturaleza de la causa del hecho obstativo (claramente "independiente y extraña a la voluntad del sujeto obligado" y la limitada capacidad de anticipación que este tipo de intrusión permite), la variada y revisión periódica del conjunto de medidas que conforman la Política de seguridad de la información de XXXXX permiten concluir que el nivel de previsión y precaución es adecuado dentro del grado de esfuerzo y coste de un ordenado y diligente comerciante.

Tal y como recogen los dos informes -técnico y pericial- obrantes en el expediente administrativo, la Compañía contaba con los siguientes medios de seguridad informáticos:

ADMINISTRACION DE JUSTICIA

• Tiene implantado sistema de gestión de seguridad de la información; basándose 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. Política de seguridad que damos por íntegramente reproducida. Dentro de esta política de seguridad, existen dos procedimientos concretos de respuesta técnica ante ataques ransomware.
Dentro de la citada política, la compañía cuenta con una "política de uso aceptable de los sistemas de información", en el que, entre otras medidas, se contemplan:
▪ Medidas de seguridad en el acceso por los usuarios a las instalaciones de la empresa, mediante tarjetas identificativas y controles de acceso.
▪ Instrucciones de seguridad en el uso de equipamiento informático, no permitiéndose manipulación del mismo por personal no autorizado -equipo de mantenimiento informático.
▪ Medidas de seguridad en el uso de cableado y conexiones.
▪ Medidas de seguridad de dispositivos móviles. ▪ Medidas de control de acceso a lógico y a sistemas de información.
▪ Medidas de construcción de contraseñas seguras de carácter intransferibles.
▪ Medidas de seguridad para uso y bloqueo de sistemas, así como de uso de software.
▪ Medidas de control y uso del correo electrónico.

• Desde el año 2017, cuanta con la certificación ISO/IEC 27001 de técnicas de seguridad de la información, otorgada por AENOR, y que es renovada anualmente mediante auditorías, siendo que, en el momento del acaecimiento del incidente de méritos, estaba plenamente vigente (Anexo VI del documento nº 6 de los acompañados a la solicitud inicial de constatación de fuerza mayor). Esta norma planta un marco de gestión para llevar el sistema de gestión.
• Certificación ISO/IEC 27001, otorgada igualmente por AENOR, vigente en el momento del acaecimiento del incidente de 52 ciberseguridad (Anexo VII del documento nº 6 de los acompañados a la solicitud inicial de constatación de fuerza mayor), que desarrolla controles específicos distribuidos en 13 capítulos que suman 133 controles.
• El modelo en el que se basa el sistema o política de gestión de seguridad es el Modelo PDCA (Planificar, Hacer, Revisar, Actual) con lo que anualmente, se hace una revisión de las medidas de seguridad que están implantadas y se promueve una mejora continúa basado en análisis de riesgos.
• La empresa tenía instalado, con las licencias debidamente renovadas en el momento de acaecimiento del ciberincidente, el Antivirus Karpersky. El equipo de servicios informáticos de la empresa, en el momento de su instalación -con carácter previo al ciberataque- pudo comprobar mediante pruebas con el ransomware como el antivirus lo detecta y elimina. En este sentido, se aportaron junto al Recurso de Alzada como documentos 13.2 y 13.4 los presupuestos de renovación del antivirus y la factura emitida.

• XXXXXX tenía contratado servicios de creación y control de puestos virtuales con la empresa Unified Cloud Services (documento nº 7 de los acompañados al Recurso de Alzada), desde fecha 1 de mayo de 2020 -data del último de los contratos que se

aportan-. En dicho contrato de prestación de servicios se contemplan la implantación de sistema de seguridad informática.
• La compañía tiene cubierto, mediante póliza de Responsabilidad Civil suscrita con AIG Europe, S.A. (documento nº 8 de los acompañados al Recurso de Alzada) Riesgos Cibernéticos por valor superior a 5.000.0000 de euros, abonándose una prima anual superior a los 146.000 euros por parte de la empresa, estando la misma vigente hasta 24 de abril de 2022.
• Cuenta, dentro de la política de seguridad de la información de la empresa, con apartado específico sobre la seguridad operativa diaria (documento nº 12 de los acompañados al Recurso de Alzada), en el que se contempla de forma específica la gestión de contraseñas de usuarios, la verificación de los acceso, modificaciones y resto de medidas de seguridad aplicables de forma continua en la empresa.
• XXXXXX, además cuenta con los servicios de Telefónica Soluciones de Informática y Comunicaciones de España, S.A.U., para la prestación de servicios de soporte y gestión de dispositivos de seguridad (documento nº 13 de los acompañados al Recurso de Alzada), relativo a los sistemas de telecomunicaciones, con un precio anual que supera los 20.000 euros (documento nº 13.3. de los acompañados al Recurso de Alzada).

Se acredita, por tanto, que la Empresa había cumplido con el nivel de diligencia debido, así se hace constar en el informe aportado en el que se recoge que la actuación y medios de seguridad de la empresa para la evitación del ataque eran los adecuados.

Cabe citar La Sentencia de la Audiencia Provincial de Valladolid de fecha 12 de septiembre de 2017 (rec. 197/2017), en la que se declara la nulidad de lo actuado porque la representación procesal no recibió la citación para el acto del juicio remitida a través del sistema Lexnet por padecer el ordenador de la procuradora el día de su envío la invasión de un virus que encriptaba los mensajes que le eran remitidos.
Argumentando que," En *su consecuencia y conforme a lo dispuesto en los arts. 162, 225.3 º y 227 de la LEC, entendemos procede decretar la nulidad de lo actuado a partir del proveído de fecha 14 de noviembre de 2016 por el que se realizaba el señalamiento del acto del juicio y se daba traslado a la parte actora de las manifestaciones del testigo-perito propuesto por esta para no comparecer a juicio. Ello por cuanto ha concurrido una causa de fuerza mayor, ajena a dicha parte y que mal pudo evitar, que ha impedido le fuera debidamente notificado dicho proveído, defecto de forma este de carácter sustancial que le ha irrogado indefensión vedándole nada menos que acudir al actor a juicio con su representación y defensa procesal para allí hacer valer las pruebas pertinentes, intervenir en las propuestas de contrario y realizar las alegaciones que estimare convenientes."*
Por tanto, no puede afirmarse como se recoge en la resolución recurrida, que el ataque por ser previsible no puede constituir causa de fuerza mayor y ello por cuanto:

- La fuerza mayor no se reduce a los supuestos de carácter imprevisible, sino también a aquellos que, siendo previsibles, resultan inevitables.

ADMINISTRACION DE JUSTICIA

- Cuando se trata de supuestos previsibles, la inevitabilidad debe analizarse ponderando, de un lado, las medidas implantadas por la empresa para la evitación del ataque y, de otro, la complejidad de la circunstancia externa que provoca la imposibilidad objetiva. Analizadas las medidas de seguridad, por consultora externa en informe forense, se constata como eran las propias de un comerciante diligente, sin que pueda imputarse comportamiento negligente y, además, si quiera se conocen medidas alternativas que hubiera podido impedir el ataque del virus, lo que revela su carácter inevitable, debiendo, por tanto, subsumirse en el supuesto de fuerza mayor.

C) Sobre la concurrencia de causa de fuerza mayor derivada del bloqueo de los sistemas informáticos de la compañía como consecuencia del sufrimiento de ataque informático mediante virus ransoware, de conformidad con lo previsto en los artículos 47.3 y 51.7 et en concordancia con lo previsto en los artículos 32 y 33.3 del Real Decreto 1483/2012 así como de la jurisprudencia que lo interpreta. acreditación de los efectos impeditivos del desarrollo de la actividad laboral.

Como tercer argumento que conduce a la Administración actuante a resolver la inexistencia de causa de fuerza mayor, se esgrime en la resolución de méritos que:

“En tercer lugar, la fuerza mayor implica la imposibilidad de trabajar, dando lugar a la suspensión del contrato de trabajo o la reducción de la jornada de los trabajadores de la plantilla afectada. Siguiendo el informe de la Inspección de Trabajo y Seguridad Social, que, con ambas partes, dicha imposibilidad “no ha quedado acreditada a la luz de las declaraciones de los trabajadores y la justificación documental aportada por la parte social. Y es que, aunque están de acuerdo en que la actividad ordinaria se ha visto afectada, 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.” Por las razones expuestas, ni se acredita documentalmente la producción del suceso, ni se acreditan los requisitos de imprevisibilidad e inevitabilidad del mismo, ni consta que se haya producido una efectiva imposibilidad de trabajar.”

Tal y como hemos expuesto, el secuestro de datos tiene una afectación obstativa en el cumplimiento de las prestaciones contractuales acordadas porque imposibilita la oportunidad empresarial de ofrecer la prestación de trabajo a las personas trabajadoras. En efecto, en la medida que se ha visto afectado el Centro de Procesamiento de Datos, en la división XXXXXX BPO, se ha producido 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.

Se reconoce por parte de CGT, y se reproduce en la resolución ahora recurrida, la existencia del ciberincidente y los efectos obstativos que el mismo ha producido sobre el normal desarrollo de la actividad laboral, que no pueden quedar desvirtuados por la manifestación de que los trabajadores “quedaron en régimen de disponibilidad para la empresa” siendo ello elemento suficiente para impedir la

ADMINISTRACION DE JUSTICIA

suspensión de sus contratos, pues lo relevante es ,la imposibilidad objetiva de prestar servicios laborales.

En el Anexo XI, del documento nº 6 obrante en el expediente administrativo, se aportan:

-Comunicaciones remitidas a los trabajadores entre fechas 4 y 8 de junio de 2021, con el siguiente tenor literal: Desde el mismo momento en que se tuvo conocimiento del ataque informático sufrido en XXXXXXX se están buscando soluciones efectivas que permitan reincorporar al mayor número de trabajadores a su puesto de trabajo y en el menor tiempo posible, como de hecho así está sucediendo.

Sin perjuicio de ello, hasta que sea posible reactivar al 100% de la plantilla, se está valorando la necesidad de regular las relaciones laborales exclusivamente de aquellos trabajadores que no estén pudiendo trabajar de una manera efectiva.

Esta regulación, en todo caso, afectaría al menor número de trabajadores posible durante el tiempo exclusivamente requerido para la recuperación de este ataque informático que ha inutilizado la mayor parte de las herramientas de trabajo disponibles.

-Comunicaciones efectuadas sobre la brecha de seguridad ocasionada, como consecuencia del ataque informático, a la Agencia Española de Protección de Datos, sobre la brecha de seguridad ocasionada como consecuencia del ciberincidente. En la misma se contempla como:
Se recibió llamada de un proveedor de servicios informáticos: Unified Cloud Services, S.L. indicando que está recibiendo tráfico de datos hacia ellos y que se trata de un ransomware.
Se ha procedido a la desconexión de los sistemas y análisis de la situación: análisis de los activos infectados (…) activación de la póliza de seguridad.

-Comunicaciones efectuadas a los clientes sobre el ciberataque producido y la imposibilidad de prestación de los servicios, se anexionaron en los términos explicitados, un total de 131 comunicaciones efectuadas a clientes acerca de la imposibilidad de continuar prestando servicios como consecuencia del ciberataque producido.

De todo lo expuesto podemos concluir que:

El ataque informático a través de un virus ransomeware en una actividad empresarial que gravita sobre una “arquitectura” esencialmente digital como la que lleva a cabo la demandante puede subsumirse en el concepto de fuerza mayor por lo siguiente:

- Primero, el origen humano del hecho obstativo no impide que pueda subsumirse un hecho imposibilitante en el concepto de fuerza mayor;

ADMINISTRACION DE JUSTICIA

- Segundo, concurre una imposibilidad absoluta y objetiva sobre una de las prestaciones esenciales empresariales del contrato de trabajo (dar ocupación efectiva);
- Tercero, existe una relación causal entre el incumplimiento de la obligación y el hecho obstativo;
- Cuarto, dado el nivel de diligencia preventiva adoptado por la demandante puede afirmarse que concurre la nota de inimputabilidad y (como mínimo) la de inevitabilidad. En este supuesto, pese a tratarse de un riesgo conocido (y, por ende, previsible), se dan suficientes elementos para entender que el nivel de diligencia empresarial para prevenir este riesgo ha sido el suficientemente elevado como para descartar que su conducta empresarial pueda calificarse como negligente (y por ello imputable), Especialmente porque las medidas que conforman la "Política de seguridad de la información" de la compañía constituyen medidas de precaución adecuadas dentro del grado de esfuerzo y coste de un "ordenado y diligente comerciante".

Como consecuencia de cuanto precede se impone la estimación de la demanda y la anulación de la Resolución de fecha 15 de julio de 2021 de La Dirección General de Trabajo declarando estimada por silencio administrativo la solicitud de declaración de fuerza mayor formulada por la empresa IXXXXX, S.A.U., como causa de la suspensión de relaciones laborales de los trabajadores afectados de su plantilla.

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

FALLAMOS

Estimamos la demanda formulada por D. JUAN JOSÉ JIMÉNEZ REMEDIOS, Letrado del Ilustre Colegio de Abogados de Sevilla, actuando en nombre y representación de XXXXXXXXXXX, 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 XXXXXXXXXXXX, S.A.U., como causa de la suspensión de relaciones laborales de los trabajadores afectados de su plantilla.

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.

ADMINISTRACION DE JUSTICIA

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 nº 0049 3569 92 0005001274 haciendo constar en las observaciones el nº 2419 0000 00 0013 22 (IBAN ES55) ; si es en efectivo en la cuenta nº 2419 0000 00 0013 22 (IBAN ES55), 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.