CIBERATAQUES COMO CAUSA DE ERTES POR FUERZA MAYOR: SU ACREDITACIÓN Y CARÁCTER INEVITABLE

Sentencia de la Audiencia Nacional de núm. 67/2023 de 26 de mayo de 2023
ECLI:ES:AN:2023:2645

Roberto Fernández Villarino*

SUPUESTO DE HECHO: La entidad mercantil ILUNION CEE CONTACT CENTER S.A.U. es una sociedad dedicada a la actividad del Contact Center que básicamente consiste en el servicio de atención de llamas telefónicas. Cuenta con cuatro centros de trabajo en Madrid, Sevilla, Santander y Oviedo. El 21-6-2021 solicitó la suspensión de los contratos de trabajo de 654 trabajadores de los 886 que componen su plantilla, La causa invocada fue el acaecimiento de una grave incidencia informática causada por el ataque de un virus del tipo ransomeware y que determinó la necesidad de tener que aislar la red con el apagado completo del Centro de Procesamiento de Datos de la empresa (CPD) para frenar la expansión.

Esta circunstancia terminó provocando el cese de la actividad de los 654 trabajadores, para los que la empresa solicitó a la Autoridad Laboral la suspensión de los contratos por la concurrencia de causa de fuerza mayor. Todo ello a través del correspondiente expediente de regulación temporal del empleo (ERTE), del que la Dirección General de Trabajo informa desfavorablemente y dicta resolución en la que acuerda declarar no constatada la existencia de dicha fuerza mayor. Frente a ella, empresa presenta recurso de alzada que no se llegó a resolver de forma expresa.

RESUMEN: La Sentencia de la Audiencia Nacional, previo reconocimiento del silencio administrativo con efectos positivos, -validación administrativa por silencio de la solicitud suspensiva de los contratos-, determina la existencia de un ataque informático que a la luz de la prueba obrante en autos, fue lo suficientemente contundente para operar como causa obstativa plena y determinantes de la imposibilidad de trabajar. En este sentido se evidencia como la empresa contaba con una serie de medios que se han valorado como suficientes para prevenir este tipo de acontecimientos.

* Profesor Asociado Derecho del Trabajo y Seguridad Social.

 Recepción original: 10.12.2023. Aceptación: 12.12.2023

INDICE

1. INTRODUCCIÓN

1.1. Posiciones de las partes ante el litigio

En la sentencia objeto de estudio, la empresa centra su argumentación en los resultados del informe de la UCO de la Guardia Civil sobre la existencia y virus padecido, sosteniendo que el ataque es causa obstativa que del desarrollo de la actividad laboral de las personas trabajadoras sobre los que se pidió la suspensión de su contrato. Por tanto considera evidenciada la relación causa efecto generada por el virus: el acaeciendo del ataque y consecuencias. Del texto de la sentencia se extrae además que está en suspenso una reclamación patrimonial al Estado como consecuencia de la denegación de la causa mayor y el perjuicio ocasionado por ello: los trabajadores no vieron suspendidos sus contratos y se les abonó el salario y se pagaron las cotizaciones a la Seguridad Social. Así mismo se hace valer que el silencio administrativo debió tener efectos positivos de la solicitud de suspensión de los contratos de trabajo.

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. El sindicato CGT se opuso 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.

1.2. Contextualización. Concepto, impactos y consecuencias de los ciberataques

Europol define a los ciberataques[1] como (sic) "Cualquier delito que solo se puede cometer utilizando ordenadores, redes informáticas y otras formas de tecnología de comunicación de la información (TIC)". Junto a esta conceptualización tan generalista aparecen otras más específicas, como la que ofrece en el informe "Ciber amenazas y tendencias del CCN-CERT[2], más orientada a las consecuencias de los mismos: "Aquella operación cibernética, ofensiva o defensiva, de la que se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas o daños y destrucción de bienes".

En cualquier caso, no es preciso tirar de pormenorizados análisis técnicos, ni siquiera de un relato actualizado de noticias sobre estos incidentes, para poder atisbar que, por una parte los ciberataques se han instalado en nuestra sociedad con carácter general, más allá del impacto sobre las empresas, afecta de igual manera a las administraciones públicas y los ciudadanos. Por otra, de la especial virulencia, gravedad y consecuencias que provocan para toda la sociedad: impacto económico, paralización de la actividad, secuestro y tráfico de datos, entre otros muchos. En este sentido, pudieran ser considerados uno de los peajes que implica la total digitalización de los usos, costumbres y estilos de vida del hombre del siglo XXI. Un fenómeno que por su complejidad, capacidad de innovación y permanente sofisticación encierra y despliega una gran variedad de manifestaciones. En este sentido, un reciente informe de la Cámara de Comercio de Madrid[3], inventariaba los distintos tipos de ataques y las consecuencias que pueden tener. Así, en primer lugar está el *ransomware*, que fue objeto de ataque en la empresa Ilunium y que tal como se expone en el hecho probado 20 de la SAN, se trata de 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. A continuación suelen pedir un "rescate" para liberar los archivos". Aunque no es una práctica nueva, este modelo de ataque ha evolucionado a lo largo de los últimos 30 años. Por otra parte está el *Adware*, se trata de un software malicioso y hostil (malware) que muestra publicidad no deseada en lugares donde no debería aparecer. A diferencia del *ransomware*, se puede eliminar con un buen antivirus. El *Phishing* es un método por el cual los delincuentes suplantan la identidad de una empresa, como un banco o una tienda en línea, para obtener tus datos personales,

[1] Europol accesible a 4-12-2023 OCTA 2018" https://www.europol.europa.eu/sites/default/files/documents/ iocta2018.pdf

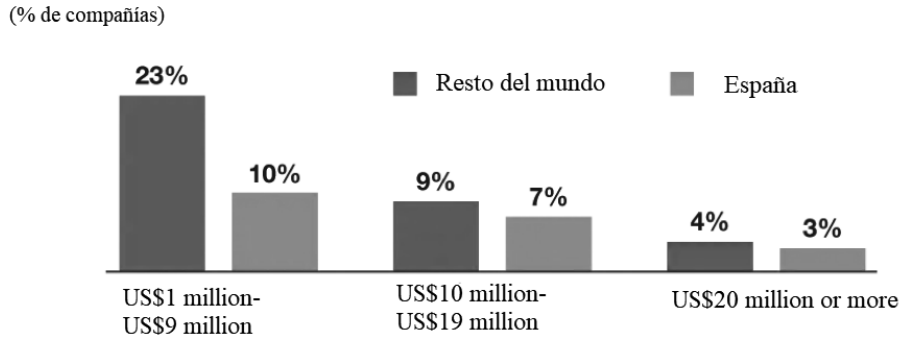
[2] Accesible a 05-12-2003 en https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-ciberamenazas-y-tendencias-edicion-2022-1/file.html

[3] Accesible a 05-12-2023 en https://ticnegocios.camaramadrid.es/servicios/tendencias/ataques-informaticos-mas-comunes-en-empresas-espanolas/

de contacto e incluso tus contraseñas. A partir de aquí logran enviar algún tipo de comunicaciones que parecen ser legítimas y te llevan a sitios web falsos que se ven idénticos a los originales.

Por lo que respecta a las consecuencias e impactos negativos de estos ataques, un reciente informe emitido por Digital Tras Survey 2024[4], elaborado por la consultora PwC, a partir de la opinión de 3.876 directivos (CISOs, CIOs, CEOs, CFOs y miembros de la alta dirección) de 71 países, y que incluyen, también, a 143 compañías españolas, concluye que el coste que para las empresas suponen de estos ataques. Así, el estudio revela que tanto el número de ciberincidentes como el impacto económico que ocasionan a las empresas han vuelto a crecer, un año más, con ataques cada vez más sofisticados. En los últimos tres años, el porcentaje de las compañías que han sufrido ciberataques críticos- o sea, con un impacto mayor al millón de dólares-, ha crecido hasta el 36%, nueve puntos más que en nuestro informe anterior. En España este porcentaje es del 20%. En cuanto a los sectores más afectados por estos ataques de gran impacto han sido los de salud, tecnología, telecomunicaciones y entretenimiento, el sector financiero y el de energía.

Coste estimado de los ciberincidentes más críticos que las empresas has sufrido en los últimos 3 años, en el mundo y en España



Fuente: Informe Digital Trus Surevey 2024 para PWC

Además preocupa especialmente entre las empresas, un incremento de los ciberataques relacionados con el alto impacto derivado del uso de la Inteligencia Artificial (IA). Así se pone igualmente de manifiesto en el citado informe, afirmándose que el 52% de las empresas -en el conjunto de la muestra y en España- aseguran que la IA va a contribuir a que se produzcan ciberataques de alto impacto en los próximos doce meses. Todo esto en un contexto en el que los incidentes de

[4] Accesible a 05-12-2023 en https://www.pwc.es/es/publicaciones/transformacion-digital/global-digital-trust-insights-2024.html

ciberseguridad crecen en número y complejidad, y en el que las compañías están aumentando año tras año sus presupuestos en ciberseguridad para contrarrestarlos.

Desde un punto de vista jurídico, estos datos de impacto vienen a reforzar todo el relato argumental de la jurisprudencia de los últimos cinco años, que han venido invocando como una de las consecuencias de especial gravedad, el relacionado con el riesgo de descargas de virus o el riesgo de ciberataques. Ello relacionado con la justificación de despidos disciplinarios por el uso ilegítimo del correo de la empresa o las visitas a webs no autorizadas. Recordemos además que esta misma circunstancia ha terminado configurando, un estricto régimen sancionador de estas conductas en los convenios colectivos de todas aquellas empresas y sectores más sensibles a estos ataques, así como la puesta en marcha de más controles y medidas preventivas[5].

Pero además de lo anterior, podemos observar la concurrencia de otro tipo de consecuencias poco conocidas (aún), y más relacionadas con los riegos de estos tipos de ataques para los derechos de las personas trabajadoras. Así la Sentencia Tribunal Superior de Justicia de Madrid (Sala de lo Social, Sección 4º) núm. 672/2021 de 5 de noviembre, en un asunto sobre solicitud teletrabajo para la conciliación de la vida familiar, se deniega la medida instada por el trabajador, entre otras por el riesgo de ataque de virus cuando la persona desempeña su actividad (teletrabaja) desde su domicilio. En este caso se trataba de una empresa que ya había sufrido previamente un ciberataque. Así en su Fundamentación Jurídica Cuarta se dice: (…) "La empresa ha acreditado las razones organizativas que le impiden conceder el disfrute del teletrabajo en los términos propuestos por la trabajadora que son riesgos de seguridad fundados en el ciberataque por el acceso al NAS en remoto fuera de la red securizada. El motivo de oposición de la empresa está acreditado y es que siendo necesario para la prestación del servicio de la recurrente como supervisora acceder al NAS y ante el ataque o incidente de seguridad producido durante el teletrabajo mediante un acceso no autorizado a los equipos técnicos de GroupEAD en Madrid, que no tuvo efectos para el sistema ni para los datos de EAD, sus servicios no pueden prestarse fuera de la sede de la empresa en estricto cumplimiento del contrato mercantil que la demandada tiene con el cliente, en el que consta que "GroupEAD prestará los servicios DOP desde sus instalaciones ubicadas en: (…)".

[5] Entre otros muchos, por ser pioneros el Convenio Colectivo Nacional de Telefónica 23-10-2019 (Accesible a 05-12-2023 en https://www.boe.es/buscar/doc.php?id=BOE-A-2019-16313), o más recientemente el convenio colectivo nacional de la Banca Privada, 17-03-2021 (accesible a 05-12-2023 en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-5003)

2. FUNDAMENTACIÓN JURÍDICA

2.1. Sobre los efectos del silencio administrativo

Por la empresa se cuestionó 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 estarse en este caso, a lo establecido en el el art. 24.1 de la Ley 39/2015 de Procedimiento Administrativo Común (en adelante LPA), determinante por silencio administrativo de la aprobación de la solicitud. Por su parte el art. 33.1 del Real Decreto 1483/2012 Reglamento de procedimientos de despidos colectivos y de suspensión y reducción de la jornada, 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. No obstante esta misma norma determina que la autoridad laboral con carácter preceptivo deberá recabar informe de la Inspección de Trabajo motivo por el cual el plazo máximo para resolver y notificar la resolución podrá suspenderse precisamente por este motivo, no pudiendo exceder la resolución un plazo superior a tres meses.

De la misma manera, el citado art. 24.1 LPA dispone que "En los procedimientos iniciados a solicitud del interesado, (…) el vencimiento del plazo máximo sin haberse notificado resolución expresa, legitima al interesado o interesados para entenderla estimada por silencio administrativo". Así la norma establece una serie de supuestos contrarios a la aplicación de esta regla general a favor del silencio positivo, resoluciones que por tanto determinan el silencio con efectos negativos. Pues bien, entre estas excepciones no se encuentra la suspensión de contratos de trabajo con causa en fuerza mayor, por lo que la Sentencia de la Audiencia Nacional en su fundamento jurídico recoge 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. Para sustentar esta argumentación cita la STS 25-1-2021 rec. 125/20 (EDJ 2021/501083), invocada por la parte demandante si bien se trataba de un supuesto aplicando el art 22.2.c del Real Decreto Ley 8/2020 de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19, lo que no es el caso.

Así pues, destacamos que SAN antes de entrar en el fondo del asunto, parte ya de la nulidad de la resolución administrativa que denegó la suspensión de los contratos por fuerza mayor.

2.2. Sobre el derecho a la ocupación efectiva y la concurrencia de causa mayor que lo impide

En efecto, como hemos comprobado uno de los efectos o consecuencias inmediatos al ataque informático, es el impacto sobre la falta real a la ocupación efectiva como derecho básico de las personas trabajadoras, conforme a lo dispuesto en el art. 4.2 a) E.T y la consecuente obligación para el empresario de llenar de contenidos esa obligación, art. 4.2 f) del E.T. A mayor abundamiento, el no acceder a los equipos informáticos infectados (por ende no desarrollar de manera efectiva su trabajo), es así mismo una recomendación expresa, a la espera de que los técnicos puedan identificar y valorar la tipología del virus y sus efectos sobre la seguridad de los datos y del resto de los sistemas de la empresa. A resultas de lo cual, conforme a la Fundamentación Jurídica Cuarta, la causa de fuerza mayor debe impactar directamente en este devenir ordinario del contrato de trabajo de tal manera que us correspondientes obligaciones de trabajar y remunerar se vean alterados por la concurrencia de supuestos fácticos que encajen en la llamada fuerza mayor. Supuesto que incidiendo en el decurso del contrato, determina su suspensión, conforme a lo establecido en el art. 47.3 E.T., o su extinción art. 51.7 E.T.

Como sabemos, el ordenamiento laboral no contempla una definición de la fuerza mayor por lo que, para su identificación, habrá de aplicarse lo establecido en el art. 1.105 del Código Civil que dispone lo siguiente: "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 las personas trabajadoras afectadas por la suspensión temporal. El hecho de comprometerse fondos públicos para atender la pérdida de salario, justifica esta intervención administrativa con el objeto de constatar la concurrencia cierta de la fuerza mayor.

2.3. Sobre los argumentos que justifican o no la existencia de la fuerza mayor

Los dos primeros argumentos de carácter fáctico que se emiten en el informe de la ITSS determinan que: "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". Dicho informe en ningún caso niega la veracidad del ataque padecido, como tampoco se niega en juicio por la Abogacía del Estado ni por parte del sindicato CGT. El ataque quedó plenamente acreditado por el informe técnico también reconocido y por el informe de la UCO, resultando especialmente relevante que parte del mismo haya sido utilizado en el propio informe de la ITSS para describir el acontecimiento determinante de la solicitud administrativa.

Sin embargo, conforme a la Fundamentación Jurídica Cuarta de la SAN el aspecto clave en estos autos es la constatación que los efectos del ataque informático hayan sido de una especial virulencia de forma tal que efectivamente hayan impedido la posibilidad de trabajar con normalidad, ha sido causa obstativa de la misma. Justificando plenamente de esta forma los efectos suspensivo sobre el contrato de trabajo típicos de la causa de fuerza mayor. Ello pese a que en la sentencia se reconoce expresamente la desigual afectación que el ataque haya podido tener sobre la generalidad de personas trabajadoras: (…) "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".

Para la acreditación de este particular a juicio de la SAN resultan esclarecedores los distintos informes de impacto sobre la actividad laboral presentados por la empresa. Más concretamente: (…) "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".

Por consiguiente, las evidencias reflejadas en esos informes le generan a la Audiencia Nacional una mayor constatación de un impacto en la actividad de la empresa, superior a los hechos contrastados en el informe de la ITSS. Así (….) "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".

2.4. Sobre la naturaleza imprevisible e inevitable de la fuerza mayor: la diligencia de la empresa

Para la Autoridad Laboral no concurría fuerza mayor porque no se daba la circunstancia de ser un acontecimiento imprevisible e inevitable al tratarse de una empresa cuyo modelo de negocio se basa precisamente en una alta utilización de los recursos informáticos y por tanto, estando o debiendo estar más preparada para este tipo de ataques. Resulta interesante la apreciación de la SAN en el sentido de no considerar a los ataques informáticos en el contexto social actual como un fenómeno imprevisible, por cuanto su existencia está a la orden del día, pero como el referido art. el art. 1105 CC terminada 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. Es por ello, que lo que debe analizarse en el presente caso es si el previsible ataque informático resultaba inevitable.

En su Fundamento jurídico sexto la sentencia refería a 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". 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. En este sentido, en el resultado probado noveno, consta que la empresa tenía implantado un Sistema de Gestión de Seguridad de la Información (GSSI), que además cuenta con la certificación ISO/IEC/27001 de técnicas de seguridad de la información otorgada por AENOR y que resulta anualmente renovada mediante auditorías. Igualmente y entre otros muchos controles, la empresa dispone de una serie de políticas, normas y procedimientos de seguridad que, ante un ciberataque, establecen pautas para actuar de forma segura en torno a la preservación de la información. Más concretamente 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.

Finalmente la SAN no aprecia en este caso, porque tampoco se alega, una conducta defectuosa en sus obligaciones preventivas en materia de seguridad informática, por lo que concluye que pese a las adecuadas que se adoptaban por la empresa el ataque tuvo lugar. Un ciberataque que resultó ser de una gran sofisticación, al punto de no haberse podido aún acreditar pese a los informes técnicos y del UCO, cuál fue finalmente, el mecanismo de entrada del virus en su Intranet.

3. CONCLUSIONES

La virulencia, impacto y asiduidad de los ciberataques en las empresas plantean ya escenarios que como en el caso de los autos enjuiciados, los han convertido en previsibles y con efectos obstativos de la capacidad de trabajar. Afectan por tanto a los derechos básicos del desempeño ordinario de las tareas y la obligación de ofrecer dicha tarea y obligan a intervenir a la administración en su faceta de amortiguación social de las suspensiones de los contratos, y por ende para contrastar la efectiva concurrencia de la causa suspensiva sobre la relación laboral.

En este escenario y a la luz de las distintas argumentaciones de las partes, podemos concluir que el fallo de la SAN nos deja al menos dos recomendaciones no poco interesantes para las empresas, en especial por cuanto ofrecen seguridad jurídica para el correcto abordaje y diligencia en torno a estos ataques. Se trata de hacer que el suceso, en la medida de lo posible resulte evitable, circunstancia que podrá acreditarse siempre que la empresa (se dedique a lo que se dedique) acredite una diligencia debida en la implementación de todas aquellas medidas, procedimientos y recursos técnicos que, de manera razonable, estén diseñadas para evitar este tipo de ataques. Todo ello contando con el grado de permanente innovación, sofisticación y complejidad inherente al mismo. Recordemos que en este caso, el origen del ataque no pudo ser aclarados ni de las propias pesquisas de la UPO. En todo caso, para las empresas con un alto grado de exposición a estos ataques, la sentencia pudiera dar pie a un posible estandarización de estos ataques como causa de fuerza mayor en empresas con alta exposición de su actividad a estas amenazas.

De tal manera que, como segunda conclusión muy vinculada a esta es que, la real amenaza y habitualidad con la que se están produciendo estos ataques que hacen necesario una permanente inversión económica de la empresa y formación a los trabajadores para evitar los peligros del uso ilegítimo de web o emails. En especial haríamos extensivo este riesgo a las personas teletrabajadores que desarrollan su actividad conectados a la IP de sus domicilios.