Los ciberataques en las empresas y sus consecuencias en el ámbito laboral

Agosto de 2024

1. ¿Qué es la ciberseguridad? ¿Qué leyes regulan la ciberseguridad en España y en la Unión Europea?

La Real Academia Española no contiene la definición de ciberseguridad. Pese a ello, podríamos definir este concepto como el **conjunto de tecnologías, prácticas y políticas utilizadas con el fin de prevenir los ciberataques o disminuir su impacto. Protegiendo los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros malware, las estafas de phishing, el robo de datos y otros ciberataques**.

La regulación de la ciberseguridad no se encuentra comprendida en una sola norma, sino que existen una serien de diferentes preceptos legales que pueden ayudar a paliar la complejidad que puede suponer un ciberataque.

En el **marco jurídico comunitario**, encontramos la Directiva de la Unión Europea 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la UE. Con el paso del tiempo, dicha norma ha sido revisada y actualizada debido a la veloz transformación digital, y la evolución de las amenazas que acarrea la misma.

Asimismo, el 7 de enero de 2024 entró en vigor el nuevo reglamento sobre ciberseguridad por el que se establecieron medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, órganos y organismos de la UE.

En cuanto a la **regulación de la ciberseguridad en nuestro país**, debemos de destacar la existencia de un Código de Derecho de la Ciberseguridad, cuyo objetivo es fijar las directrices generales en el uso seguro del ciberespacio a través del impulso de una visión integradora que garantice la seguridad y el progreso en España. El código menciona numerosas normas entre ellas:

- La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que regula los principios y organismos clave, así como las funciones que deberán desempeñar para la defensa de la Seguridad Nacional.

- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

- La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

- La Orden TIN/3016/2011, de 28 de Octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

2. El ciberataque como causa de ERTE

Una reciente **sentencia** a tener en cuenta en este ámbito es la **del 11 de junio de 2024, en la que el Tribunal Supremo declaró que un ciberataque es un motivo válido y de fuerza mayor para realizar un Expediente de regulación temporal de empleo (ERTE).**

Para comprender el fallo de la sentencia, en primer lugar, tendremos que considerar los hechos acontecidos. El día 4 de junio de 2021 a las 5:15 am, la empresa Ilunion Contact Center recibió una incidencia alertando de que los Virtual Desktop Infrastructure (tecnología de virtualización de escritorio que almacena un sistema operativo en un servidor centralizado de un centro de datos) no funcionaban correctamente.

Detectada la mencionada incidencia se contacta con la compañía externa que da soporte al grupo Ilunion, la cual detecta que un servicio de Base de Datos tampoco funciona correctamente, además de que se estaban generando tráfico de datos hacia ellos y se sospechaba que se trata de un virus ransomware. A las 6:40 am se procede a cortar las comunicaciones con todas las sedes de la división Contact Center BPO para evitar la distribución del virus, e inmediatamente se informa del incidente a Grupo Ilunion.

El mismo día en el que se detecta el incidente, esto es, el 4 de junio de 2021, se remite comunicación a todos los clientes informándoles de la existencia de un posible incidente de ciberseguridad. Asimismo, se informa inmediatamente a los trabajadores y a su representación unitaria de la imposibilidad de prestar servicios en las unidades afectadas, por la inutilización de las computadoras, impresoras, escáner, etc. así como consecuencia del riesgo existente en materia de seguridad de la información de no adoptarse las mencionadas medidas y la cesión de la actividad en las unidades afectadas.

Por ello, la empresa, en fecha 21 de junio de 2021, se ve obligada a efectuar, ante la Dirección General de Empleo del Ministerio de Trabajo y Economía Social, **solicitud de constatación de fuerza mayor, en que se fundaba expediente de regulación temporal de empleo que contemplaba medidas suspensivas y de reducción de jornada, que afectaban a un total de 1.192 personas trabajadoras de la empresa,** distribuidos en sus centros de trabajo de Madrid, Barcelona, Sevilla y Logroño. Solicitud que fue denegada el 19 de julio de 2021.

Mientras que el Estado decidió impugnar la aplicación del ERTE ya que consideraba que un ciberataque era previsible debido a que el desarrollo empresarial se realizaba por medios digitales, el Tribunal Supremo entiende que ***"no es admisible, pues el hecho de que sea previsible un ataque de este tipo en una empresa cuyos medios materiales son esencialmente digitales, como lo son los ordenadores, no lo convierte en evitable".*** Por otro lado, el Alto Tribunal se apoya en el artículo 1.105 del Código Civil, con el fin de justificar la cuestionabilidad de la existencia de fuerza mayor en el suceso, ya que el precepto no exige que sea un suceso natural, pudiendo ser de otro tipo *"atendida la realidad social en la que nos hallamos, una sociedad tecnológica, donde los sucesos pueden ser provocados por la acción*

del hombre". Además, se detalla que *"la principal diferencia entre una causa de fuerza mayor y otra de tipo objetivo técnica no está en la causalidad natural de la primera y la humana en la segunda, sino en el hecho de que la fuerza mayor es un suceso externo, ajeno a la voluntad de la empresa y de carácter extraordinario, y la segunda es una causa introducida, favorecida o exigida por las circunstancias, pero siempre ordinaria y voluntaria"*.

En relación con las **medidas de seguridad**, se declara que la empresa había previsto la posibilidad de recibir un ciberataque ya que disponía de las medidas de seguridad necesarias y suficientes y pese a ellas, el mismo no pudo ser evitado. Apoyándose en el informe técnico aportado y señalando la complejidad que supone recibir este tipo de malware, aunque la empresa disponga de una protección*, "es imposible mantener una protección total ante una incidencia de este tipo"*.

Por lo que se refiere a **la prestación de servicios de las personas trabajadoras afectadas por el ciberataque,** *"el CPD se apagó por completo y se procedió a cortar las comunicaciones con todas las sedes de la división Contact Center BPO para evitar la distribución del virus, mientras se desarrollaba la investigación forense del escenario identificado"*. Es decir, se procedió a la interrupción total del tráfico saliente desde la organización hacia otros posibles servicios, debido a que la red fue completamente aislada. Asimismo, se emitieron notificaciones a los clientes informando sobre el ciberataque ocurrido y la consiguiente imposibilidad de prestación de los servicios. En consecuencia, únicamente algunos empleados pudieron continuar con la prestación de sus servicios. Cabe señalar que el número de trabajadores incluidos en el Expediente de Regulación Temporal de Empleo (ERTE) fue inferior al de los equipos afectados, y considerablemente inferior al total de la plantilla de la empresa.

3. ¿Se puede despedir a las personas trabajadoras que caen en una estafa informática?

Para dar respuesta a esta cuestión, analizamos la **sentencia de 22 de junio de 2021 del Tribunal Superior de Justicia de la Comunidad Valenciana, en la que declara procedente el despido de un alto cargo de una empresa tras haber caído en una estafa.**

La trabajadora recibió una llamada telefónica de un sujeto que se identificaba como asesor fiscal de una consultora reconocida y posteriormente le informó de que se encontraba asesorando a la empresa en el proceso de adquisición de una sociedad extranjera. Tras varios correos electrónicos entre la trabajadora y el supuesto asesor fiscal, en los cuales se incluían documentos en los que constaban firmas de los apoderados de la empresa, la trama culminó con la autorización de pago de un importe superior a los 4 millones de euros a cuentas bancarias de diferentes países.

La Sala declaró que la conducta de la trabajadora al facilitar los documentos firmados por dos de sus superiores jerárquicos *"constituía una grave transgresión de la buena fe contractual que ha ocasionado además un perjuicio sustancial para la empresa demandada".* Asimismo, se

dicta que la conducta de la trabajadora comprometía la reputación de otros trabajadores de la compañía, viéndose involucrados en la estafa sufrida por la empresa, a través de la utilización de sus firmas.

La Sala de lo Social del TSJ de la Comunidad de Valencia también consideró que la entrega de los documentos solicitados por los estafadores no resultaba necesaria y carecía de justificación. Por lo que el fallo de la sentencia **declaraba que la sanción de despido impuesta a la trabajadora era proporcionada ante la gravedad del incumplimiento contractual, basándose en el artículo 54.2 del Estatuto de los Trabajadores, y ratificándose en la procedencia del despido.**

4. Valoración crítica y conclusiones

Tras el análisis de las sentencias expuestas anteriormente quedan reflejados los complejos supuestos en los que se puede ver incursa una empresa, así como una persona trabajadora al recibir un ciberataque.

Son numerosas las empresas, así como organismos públicos los que reciben este tipo de ataques, amenazados por la constante evolución de la tecnología y de su adaptación y desarrollo en dicho panorama. Es por ello por lo que la formación continua en ciberseguridad para todos los empleados es crucial para crear una primera línea de defensa eficaz. Los ciberataques a menudo explotan errores humanos y, la capacitación regular en ciberseguridad ayuda a los empleados a reconocer amenazas y a tomar decisiones informadas para proteger los activos digitales de la empresa.

Asimismo, es indispensable que las empresas implementen políticas de ciberseguridad robustas y que actualicen continuamente sus sistemas de defensa para enfrentar nuevas amenazas.

En definitiva, la importancia de los ciberataques en las empresas subraya la necesidad inminente de adoptar una postura de seguridad proactiva. La formación en ciberseguridad debe ser una prioridad para todas las empresas, no solo para protegerse contra amenazas actuales, sino también para estar preparadas para futuros desafíos en el cambiante panorama de la ciberseguridad.

Lucía Grasa Royo

Abogada Laboralista – Employment Lawyer

derecho.laboral@mazars.es