

LA IMPORTANCIA DE UNA ADECUADA GOBERNANZA DE LA SEGURIDAD DIGITAL EN LA EMPRESA A LA LUZ DE LA SENTENCIA DE LA AUDIENCIA NACIONAL 37/2022

9 de abril de 2020

Vicente Moret Millás
Of Counsel
Cristina Durante Del Barrio
Associate Lawyer
Andersen

A pesar de que Ilunion sufrió un ataque de ransomware muy grave, las actuaciones que en material de gobernanza de la seguridad digital había ido desplegado en los últimos años, le permitieron, contra el criterio del Ministerio de Trabajo, ver estimada su pretensión de considerar ese ciberataque como causa justificativa de la fuerza mayor necesaria para iniciar un expediente de ERTE.

Ello sólo fue posible porque, como dice la sentencia, el empresario había desplegado todas las medidas y políticas en materia de ciberseguridad necesarias para demostrar la diligencia debida para proteger a la empresa.

- ❑ **Ilunion Contact Center**, es una empresa que desempeña su actividad en el sector del contact center o telemarketing. El 4 de junio de 2021 sufrió un **ataque de ransomware RYUK** que motivó el corte total de las comunicaciones y la actividad para evitar la distribución del virus. Ello causó la **imposibilidad de prestar servicios** en las unidades afectadas, por la inutilización de las computadoras, más de 1.200, impresoras, escáner y otros dispositivos.
- ❑ Las **medidas** adoptadas para la contención y recuperación del entorno afectado por el incidente fueron las **adecuadas**, llevándose a cabo de forma ágil y mitigando por lo tanto considerablemente el riesgo de potenciales impactos adicionales.
- ❑ Como consecuencia de lo anterior **Ilunion solicitó a la autoridad laboral el inicio de un ERTE** para los trabajadores motivado por un ataque de ransomware que constituye una causa de fuerza mayor de las contempladas en la norma para justificar este procedimiento laboral.
- ❑ El Ministerio de Trabajo **denegó a Ilunion el ERTE** alegando que al ser previsible la posibilidad de sufrir un ataque informático a gran escala, no concurre la circunstancia de imprevisibilidad que motiva la fuerza mayor. Es decir, que se sostiene que la empresa no tomó las medidas adecuadas para prevenir el incidente y por ello no hay causa que justifique el procedimiento de ERTE.
- ❑ No obstante, la **Audiencia Nacional en la Sentencia 37/2022**, señala que la demanda **debe ser estimada** por la **conurrencia de fuerza mayor** en la que se funda el expediente de regulación temporal de empleo y que justifica la suspensión de jornada laboral planteada por la empresa.

- ❑ Sobre todo, **la sentencia aprecia la conurrencia de causa de fuerza mayor como consecuencia del ransomware**, afirmando que el ataque informático se traduce en el "secuestro"

de la información clave de la empresa, afectando de forma determinante a su operatividad, y por ello, puede ser calificado como un supuesto de fuerza mayor.

- ❑ En este supuesto, concluye la AN, 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".
- ❑ Alega que las medidas que conforman la Política de seguridad de la información de Ilunion permiten concluir que el nivel de previsión y precaución es adecuado. Se acredita, por tanto, que la Empresa había cumplido con el **nivel de diligencia debido**.
- ❑ En este sentido, como señala la sentencia, es concluyente la existencia de **una política de seguridad** de la información en la empresa que **valora como sólida y completa**:
 - Existencia de un Sistema de Gestión de Seguridad de la Información (SGCI) que se revisa anualmente.
 - Certificación ISO/IEC 27001 y Certificación ISO/IEC 27002.
 - Política de Seguridad (PO01) de la cual se derivan normas que cubren todos los capítulos que se desarrollan en la ISO 27002.
 - Activos e información inventariados y controlados.
 - Control de acceso a los sistemas basados en el principio de mínimo privilegio.
 - Controles con exigencia de contraseñas complejas; revisión periódica de los permisos y privilegios de los usuarios; segmentación de redes; realización periódica de copias de seguridad y almacenamiento en lugares seguros, y otras.
 - Apoyo en varias empresas de soporte especializadas
 - Una póliza de seguro de ciberriesgo.
- ❑ Dado el nivel de diligencia preventiva adoptado por Ilunion, sostiene la sentencia, 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**.

Como consecuencia de lo anterior, Ilunion ve estimada su demanda y se produce la anulación de la resolución de Dirección General de Trabajo que negaba el expediente de regulación temporal de empleo.

Madrid; 9 de abril de 2022

