UN ANÁLISIS BREVE DE LA NUEVA LEY REGULADORA DE LA PROTECCIÓN DE LOS "WHISTLEBLOWERS" EN MATERIA DE CIBERSEGURIDAD

ANÁLISIS FLASH

VICENTE MORET

CRISTINA DURANTE

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

Febrero 2023

Calle de Caracas, 6, Planta Baja, 28010, Madrid.

Contacto

+34 914252577 /609484940

www.fundacionesys.com

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

ANÁLISIS FLASH

VICENTE MORET

Letrado de las Cortes Generales, abogado asesor en Andersen, experto en negociación ciber, profesor adjunto en iE Law School. Secretario del Patronato de la Fundación ESYS.

CRISTINA DURANTE

Asociada del Departamento Legal Tech, ciberseguridad, en Andersen.

Febrero 2023

El pasado 16 de febrero se aprobó la Ley 2/2023, de 20 de febrero, que regula la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. Esta Ley traspone la Directiva 2019/1937 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

En materia de ciberseguridad, una de las novedades más importantes es la inclusión de la normativa NIS1 y NIS 2, así como el Reglamento DORA, por la que se incluye y amplía la protección de las personas que informen sobre infracciones referidas a la privacidad, los datos personales así como la seguridad de las redes y los sistemas de información.

Este hecho significa que las empresas deberán regirse por el cumplimiento de esta norma y, por tanto, los tipos de actores que quedarán protegidos para iniciar el procedimiento de denuncia en este ámbito se amplía y serán los siguientes:

1. Los empleados;
2. Los accionistas;
3. Los miembros de los órganos de administración y dirección;
4. Personas que trabajen para, o bajo, la supervisión y dirección de contratistas, subcontratistas y proveedores.

En particular, con esta nueva ley se crean dos sistemas de información por los que se podrá canalizar el procedimiento de denuncia en el caso de que se cometa una infracción de la normativa amparada, también incluyendo las Directivas NIS1 y NIS2 así como el reglamento DORA:

1. Un Sistema interno de información, del cual deberán disponer todas las empresas de más de 50 trabajadores como máximo antes de junio de 2023.
2. Un Sistema externo de información, regido por la Autoridad Independiente de Protección del Informante, y cuyas competencias serán estatales.

Estos mecanismos suponen que, ante infracciones en el ámbito de la seguridad de las redes y los sistemas de información, o la privacidad y los datos personales, el denunciante quedará protegido ante cualquier tipo de represalia, como es la suspensión del contrato de trabajo, el despido la extinción de la relación laboral, los daños reputacionales, la denegación de formación o licencias, y cualquier tipo de discriminación. Las sanciones podrán ascender

hasta los 300.000 euros cuando se cometan infracciones por parte de personas físicas, y hasta de 1 millón de euros por personas jurídicas. La incorporación de esta nueva ley deberá realizarse antes de junio de 2023.

En conclusión, la ciberseguridad ha ampliado su espectro de gobernanza y ha adquirido una nueva capa de protección de los denunciantes, o whistleblowers. Este ámbito resulta cada vez de mayor relevancia e interés, considerando los riesgos para la seguridad de la información que pueden proceder de manera externa a una entidad, pero también de manera interna, sea desde el ámbito del empleado, de dirección, de los sistemas IT/OT o de figuras como el insider trading, entre otros.