AUGUSTAABOGADOS

ALERTA INFORMATIVA
14 de enero de 2026

BRECHA DE SEGURIDAD EN ENDESA: ¿CÓMO PUEDEN PROTEGERSE LAS EMPRESAS ANTE ESTE TIPO DE CIBERATAQUES?

Ciberseguridad y privacidad en la hoja de ruta de las empresas

La inversión en ciberseguridad y gobernanza de la privacidad deben ser imprescindible en la hoja de ruta de las empresas.

El reciente ciberataque sufrido por la empresa energética Endesa Energía, que ha afectado a miles de clientes exponiendo sus datos personales, pone de relevancia una vez más la responsabilidad de las empresas en la gestión de la seguridad de la información y del cumplimiento de las obligaciones establecidas en el Reglamento General de Protección de Datos (RGPD). El acceso indebido a datos personales y su filtración al público en general puede conllevar riesgos para las personas titulares de los datos como el robo de credenciales o la suplantación de identidad.

Este tipo de incidentes que vulneran los principios de confidencialidad, integridad incluso disponibilidad (descritos en el artículo 5 del RGPD) y que sacan a la luz una posible falta de responsabilidad proactiva por parte de la empresa en el cumplimiento de las obligaciones del RGPD, tienen graves consecuencias también para las empresas atacadas.

Barcelona
Vía Augusta, 252, 4.ª
08017 Barcelona
T +34 933 621 620 ▫ **F** +34 932 009 843

Madrid
Antonio Maura, 18, 2.ª
28014 Madrid
T +34 911 592 323 ▫ **F** +34 911 592 322

Brussels (with IUROPE)
Avenue de Cortenbergh, 52
1000 Brussels (Belgium)
T +32 2 808 69 41

augustaabogados.com

El daño a la reputación corporativa y las sanciones elevadas que prevé la normativa, de hasta el 4% de la facturación global anual o 20 millones de euros, son motivo suficiente para considerar la ciberseguridad y privacidad como una prioridad.

Priorizar e invertir

Los expertos dicen que es prácticamente inevitable ser atacado en algún momento. Sin embargo, lo que sí pueden evitar las empresas es que las consecuencias de un posible ataque sean muy graves, tanto para el afectado como para la entidad atacada. Por este motivo, las empresas deben poner los medios necesarios para tener un nivel de cumplimiento óptimo en protección de datos y ciberseguridad. Esto se traduce en el cumplimiento de obligaciones enfocadas a proteger los datos personales y evitar que las ciber amenazas acaben materializándose.

Recomendaciones

Las empresas deben garantizar un nivel de seguridad adecuado al riesgo y unos procesos de tratamiento de datos personales con garantías suficientes.

Para ello, es imprescindible:

1. Planes de adecuación al RGPD y normativas de seguridad de la información.
2. Integrar la ciberseguridad y la privacidad en los procesos corporativos.
3. Programas de formación para empleados y proveedores.
4. Protocolos para la correcta gestión de incidentes.
5. Contratos con proveedores que incluyan medidas y garantías de ciberseguridad.

6. Análisis de riesgos y pruebas de penetración periódicos para detectar posibles amenazas.
7. Controles o auditorías para evaluar grado de cumplimiento e implementar mejoras.

Conclusión

Las brechas de seguridad ocurren, la gravedad de las consecuencias de una brecha está, en gran medida, bajo el control de las empresas.

La proactividad en la correcta gestión de los datos personales y la información corporativa debe ser una prioridad para las empresas.

Las empresas deben entender que la dedicación de recursos en implementar correctamente las medidas asociadas a la ciberseguridad y la privacidad no es solo una obligación legal, sino también una medida estratégica.

Júlia Bacaria. Socia
Departamento TMT | Augusta Abogados
j.bacaria@augustaabogados.com