19/02/2025

La figura del guardián de los datos se agiganta en las empresas

En un contexto de ciberataques cada vez más sofisticados y de presión regulatoria, el trabajo de los DPO adquiere un enfoque estratégico y cobra una nueva dimensión



En un entorno donde la regulación sobre privacidad se endurece y los ciberataques son cada vez más sofisticados, el delegado de protección de datos (DPO) ha ganado un peso estratégico dentro de las empresas. Lo que comenzó como un rol técnico centrado en el **cumplimiento normativo** se ha convertido en una pieza clave para la gestión de riesgos y la confianza digital. La presión regulatoria y la creciente preocupación por la seguridad de la información han ampliado sus funciones, hasta convertirlo en un perfil indispensable en el actual escenario corporativo.

Este cambio ha sido especialmente evidente desde la entrada en vigor del GDPR en 2018, explica Noemí Brito, socia responsable del área de IT, IP y legal operations en KPMG Abogados. En un principio, el DPO se limitaba a supervisar el tratamiento de datos y garantizar el cumplimiento normativo, apunta Brito. Con el tiempo, sin embargo, su función ha adquirido un enfoque más estratégico, en el que participa activamente en la gestión de riesgos y en la adaptación de las empresas a un entorno regulatorio en constante evolución, añade.

En este nuevo escenario, el DPO ha ampliado su ámbito de actuación más allá del cumplimiento normativo, señala Brito. Su labor abarca desde la definición de políticas de privacidad hasta la gestión de riesgos y la formación interna. En un contexto de **transformación digital**, su función es clave para garantizar que la innovación respete la privacidad y los derechos de los usuarios, añade. Esta evolución ha llevado a los delegados de protección de datos a alejarse de un enfoque estrictamente legalista, explica Marta Cañas, profesora del Máster en Ciberseguridad en la Escuela Técnica Superior de Ingeniería de la Universidad Pontificia Comillas (Comillas ICAI). En lugar de limitarse a interpretar la normativa para determinar qué está permitido y qué no, el DPO actual trabaja en colaboración con las áreas de negocio para identificar soluciones dentro del marco legal, dicen desde la universidad.

Más que un garante del cumplimiento, el DPO se ha consolidado como un **activo estratégico** en las empresas, señala Tania González, responsable de la oficina de protección de datos de NTT DATA. Su labor abarca la creación de una cultura corporativa basada en la transparencia y la seguridad, explica. A través del asesoramiento y la formación, refuerza la confianza de empleados, directivos y clientes, añade.

Comunicar y negociar

Más allá del conocimiento normativo, un DPO eficaz debe contar con habilidades clave para gestionar la privacidad en una organización, señala Juan José Sánchez, profesor de la Universidad Alfonso X. La comunicación es fundamental para traducir conceptos legales y técnicos en un lenguaje comprensible para toda la empresa, dice. También debe saber negociar, equilibrando las exigencias regulatorias con las necesidades del negocio y gestionando resistencias internas, comenta. En liderazgo, su papel es impulsar una cultura de protección de datos y fomentar la privacidad desde el diseño, explica Sánchez. Además, el análisis riguroso le permite evaluar riesgos tecnológicos y revisar contratos con precisión. Su independencia y ética garantizan el cumplimiento sin concesiones, concluye.

Sin embargo, su papel no está exento de desafíos. La digitalización y el avance de la IA han multiplicado las responsabilidades del DPO, que ahora debe enfrentarse a una gestión de datos cada vez más compleja, señala Brito, de KPMG. Con el crecimiento exponencial de la información, su labor ya no se limita a la privacidad, sino que se extiende a la **gobernanza de datos**. Su reto es garantizar un equilibrio entre protección y uso legítimo, asegurando que las empresas adopten estrategias eficaces sin comprometer la seguridad.

El desarrollo de la inteligencia artificial (IA) añade una capa de complejidad, advierte Brito. Los algoritmos dependen de grandes volúmenes de datos, lo que plantea interrogantes sobre privacidad y cumplimiento normativo. Los DPOs deben supervisar que estas tecnologías operen dentro del marco legal y evaluar su impacto ético. Para ello, su trabajo requiere una coordinación estrecha con los equipos de TI, legal y cumplimiento, asegurando un enfoque integral en la gestión de datos.

Una buena gestión de los datos es clave para afrontar estos retos y garantizar que la IA funcione con fiabilidad, señala Santiago Vázquez-Graña, DPO de Capgemini España.

Para que la IA sea fiable, las empresas deben garantizar que los datos con los que entrenan sus modelos sean precisos, seguros y respeten la privacidad, añade. Una gestión adecuada no solo mejora la calidad de los algoritmos, sino que también refuerza la confianza en su uso. Esto implica aplicar controles rigurosos en todo el ciclo de vida del dato, desde su recopilación hasta su almacenamiento y procesamiento, explica.

Enfoque proactivo

El cumplimiento normativo en IA requiere un enfoque proactivo, apunta Vázquez-Graña. No basta con garantizar la protección de datos, sino que es necesario incorporar tecnologías como la anonimización, el cifrado homomórfico o el aprendizaje federado para minimizar riesgos. Evaluar el impacto de cada proyecto y establecer límites claros en el uso de la información es clave para desarrollar modelos de IA que sean no solo eficientes, sino también éticos y confiables, concluye.

Estos perfiles están al alza ante la creciente regulación y la necesidad de proteger datos sensibles, dice José Muñoz-Seca, director del área tax & legal de LHH / Grupo Adecco. Las empresas buscan evitar sanciones, fortalecer su reputación y garantizar una gestión ética, con especial foco en sectores con mayores exigencias regulatorias, añade.

Desde la Universidad Pontificia de Comillas destacan que, en cuanto a regulación, las empresas europeas deben priorizar el cumplimiento del GDPR y las normativas locales antes de evaluar el impacto de leyes extranjeras como la PIPL en China o el Clopujd Act en EE.UU. Estas regulaciones externas tienen un alcance variable según el servicio o la operación que se realice en cada país, explican.

El DOP juega un rol esencial en este contexto regulatorio, apunta Juan José Sánchez, director del máster universitario online en ciberseguridad de la Universidad Alfonso X. Aunque no existe una titulación obligatoria, formaciones en derecho, ciberseguridad o ingeniería, junto con másters especializados, son altamente valoradas.

Vías de formación

Además, certificaciones como el CIPP/E, CIPM o el esquema de certificación de la AEPD aseguran competencias clave en seguridad, privacidad y cumplimiento normativo, pilares para destacar en un entorno cada vez más complejo, comenta.

Las cualificaciones y certificaciones, combinadas con conocimientos en normativas como el RGPD o NIS2 y habilidades en gobernanza de datos, permiten a los DPOs responder a las crecientes exigencias de la protección de datos, concluye Sánchez. En un panorama marcado por **regulaciones cada vez más estrictas**, su papel es crucial para garantizar la seguridad, minimizar riesgos y generar confianza tanto en las empresas como en los usuarios.

En este contexto, el DPO se ha consolidado como un pilar estratégico para las empresas, concluye Noemí Brito, de KPMG. Su función va más allá del cumplimiento normativo, integrándose en la estrategia empresarial para hacer de la privacidad un valor diferencial. La transparencia en la gestión de datos refuerza la confianza de clientes y socios, al tiempo que aporta una ventaja competitiva en sectores altamente regulados. En un entorno marcado por la digitalización y el **auge de la IA**, su papel es clave para garantizar una gobernanza eficaz y minimizar riesgos. En un marco normativo en constante evolución, el DPO no solo protege, sino que impulsa la innovación y la sostenibilidad empresarial.

Fuente: https://www.abc.es/

LINK DE LA NOTICIA